DEVICE AND METHOD FOR INFORMATION PROCESSING AND STORAGE MEDIUM

Publication number: JP2002259605

Publication date: 2002-09-13

Inventor: IINO YOICHIRO

Applicant: SONY CORP

Classification:

- international: ***G06F12/14; G06F21/00; G06F21/24; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/00; H04L29/06; H04L29/08; H04N7/167; H04N7/24;*** **G06F12/14; G06F21/00; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G09C1/00; G11B20/00; H04L29/06; H04L29/08; H04N7/167; H04N7/24;** (IPC1-7): G06F17/60; G06F12/14; G09C1/00

- European: H04L29/08N5; G06F21/00N7D; G06Q20/00; G06Q30/00A; G11B20/00P; H04L29/06S4; H04L29/06S8D1; H04L29/06S8G; H04L29/06S12A; H04N7/167D; H04N7/24C12P

Application number: JP20010050781 20010226

Priority number(s): JP20010050781 20010226

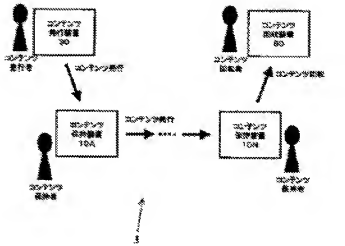
Also published as:

EP1365536 (A1)
WO02069557 (A1)
US2005262321 (A1)
CN1520655 (A)

Report a data error here

Abstract of **JP2002259605**

PROBLEM TO BE SOLVED: To hold and protect digital information on durable hardware. SOLUTION: A system which moves the digital information without allowing its duplication by using a hardware mechanism generates a record regarding the movement of the digital information, i.e., a transfer history. When the digital information is collected later, what point of time the digital information is copied by altering hardware can be specified by analyzing the transfer history. The data structure of the transfer history is a nesting structure and then while the calculation quantity for transfer history inspection needed for transfer of each time is made constant irrelevantly to the frequency of transfer, tolerance to the alteration of the transfer history by an illegal user in the middle of distribution is also actualized.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－259605
（P2002－259605A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ０６Ｆ　17/60	１４２	Ｇ０６Ｆ　17/60	１４２	５Ｂ０１７
	３０２		３０２Ｅ	５Ｊ１０４
	５１２		５１２	
12/14	３２０	12/14	３２０Ａ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	

審査請求　未請求　請求項の数30　ＯＬ　（全 28 頁）

(21)出願番号　特願2001－50781(P2001－50781)

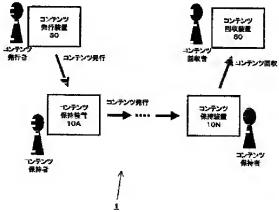
(22)出願日　平成13年２月26日(2001.2.26)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　飯野　陽一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

Ｆターム(参考)　5B017 AA08 BB00 CA16
5J104 AA09 LA03 LA06

(54)【発明の名称】　情報処理装置及び方法、並びに記憶媒体

(57)【要約】
【課題】　耐久性のあるハードウェア上にデジタル情報を保持して保護する。
【解決手段】　ハードウェア機構を用いて複製を許さずデジタル情報を移動させるシステムにおいて、デジタル情報の移動に関する記録すなわち譲渡履歴をとる。後にデジタル情報を回収したときに、譲渡履歴を解析すれば、どの時点でハードウェアの改変によってデジタル情報の複製が行われたかを特定することができる。譲渡履歴のデータ構造を入れ子構造とすることで、各譲渡時に必要な譲渡履歴検査のための計算量を譲渡回数によらない一定値としながら、流通途中での不正者による譲渡履歴の改竄に対する耐久性をも実現する。



【特許請求の範囲】

【請求項１】装置間でコンテンツを交換する情報処理装置であって、

コンテンツ及びコンテンツの譲渡履歴を送信及び／又は受信する通信手段と、

装置固有の情報を保管する固有情報保持手段と、

コンテンツを交換する相手側の装置と相互認証する認証手段と、

コンテンツを保持するコンテンツ保持手段と、

コンテンツの譲渡履歴を管理する譲渡履歴管理手段と、

を具備することを特徴とする情報処理装置。

【請求項２】前記認証手段は、コンテンツを交換する相手側の装置と互いの電子署名の認証を行う、ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】前記通信手段は、前記認証手段により認証に成功した相手側の装置に対してコンテンツを送信する、ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】前記コンテンツ保持手段は、前記通信手段により送信した後のコンテンツを消去する、ことを特徴とする請求項１に記載の情報処理装置。

【請求項５】前記譲渡履歴管理手段は、

コンテンツ受信時にはノンスを発生し、

コンテンツ送信時には、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側が発生したノンスＴＮ、並びにコンテンツの譲渡履歴全体に対する電子署名ＴＳＧを含んだ新規レコードをコンテンツの譲渡履歴に追加する、ことを特徴とする請求項１に記載の情報処理装置。

【請求項６】前記譲渡履歴管理手段は、コンテンツ受信時に、コンテンツの譲渡履歴の最後のレコードにコンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴に対するコンテンツ送信側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査し、さらにコンテンツが持つ固有情報がコンテンツ送受信側で一致するか否かを検査する、ことを特徴とする請求項５に記載の情報処理装置。

【請求項７】前記譲渡履歴管理手段は、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタＣＡの公開鍵P_{ca}を用いて暗号化したもので置換する、ことを特徴とする請求項５に記載の情報処理装置。

【請求項８】前記通信手段は、前記認証手段により認証に成功した相手側の装置から、前記譲渡履歴管理手段により譲渡履歴を確認した後にコンテンツを受信する、ことを特徴とする請求項１に記載の情報処理装置。

【請求項９】複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する情報処理装置であって、

前記譲渡履歴は、

コンテンツ固有の情報ＴＩＤと、

コンテンツを譲渡する度に追加されるレコードと、を含み、

前記情報処理装置は、

コンテンツ及び譲渡履歴を受信する通信手段と、

譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出手段と、を具備することを特徴とする情報処理装置。

【請求項１０】前記不正検出手段は、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信したことに応答して、不正の検出を開始する、ことを特徴とする請求項９に記載の情報処理装置。

【請求項１１】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、

前記不正検出手段は、譲渡履歴に含まれる各レコードの電子署名を検証して、整合しない電子署名をしたコンテンツ送信側の装置を不正者として特定する、ことを特徴とする請求項９に記載の情報処理装置。

【請求項１２】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、

前記不正検出手段は、譲渡履歴の先頭レコードに含まれるＳＩＤがコンテンツを発行する所定の装置を示していない場合には、該ＳＩＤによって識別される装置を不正者として特定する、ことを特徴とする請求項９に記載の情報処理装置。

【請求項１３】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、

前記不正検出手段は、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信した場合には、各コンテンツが持つ譲渡履歴を比較して、同じコンテンツ固有情報ＴＩＤを持つコンテンツに付随する譲渡履歴が正しく先頭のコンテンツ送信側の装置固有情報ＳＩＤのレコードから始まり且つ途中まで同一内容のレコードを持つが異なり始める枝分かれレコードを探索して、該枝分かれしたレコード中のコンテンツ送信側の装置固有情報ＳＩＤによって識別される装置を不正者として特定する、ことを特徴とする請求項９に記載の情報処理装置。

【請求項１４】前記不正検出手段は、

譲渡履歴の各レコードが所定の管理センタＣＡの公開鍵P_{ca}で暗号化されている場合には、譲渡履歴に含まれる各レコードを最新のものから順に該管理センタＣＡの秘

鍵S_{CS}によって復号化して検査し、
正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを特徴とする請求項９に記載の情報処理装置。
【請求項１５】他の装置にコンテンツを譲渡する情報処理方法であって、
コンテンツ譲受側の装置と相互認証するステップと、
コンテンツの譲渡履歴を更新するステップと、
コンテンツの譲渡履歴をコンテンツ譲受側の装置に送信するステップと、
前記相互認証並びにコンテンツ譲受側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲受側の装置に送信するステップと、を具備することを特徴とする情報処理方法。
【請求項１６】前記のコンテンツの譲渡履歴を更新するステップでは、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ受信側が発生したノンスＴＮ、並びにコンテンツの譲渡履歴全体に対する電子署名ＴＳＧを含んだ新規レコードをコンテンツの譲渡履歴に追加する、ことを特徴とする請求項１５に記載の情報処理方法。
【請求項１７】他の装置からコンテンツを譲受する情報処理方法であって、
コンテンツ譲渡側の装置と相互認証するステップと、
コンテンツ譲渡側の装置にノンスＴＮを送信するステップと、
コンテンツの譲渡側の装置からコンテンツの譲渡履歴を受信するステップと、受信した譲渡履歴を検査するステップと、
コンテンツ譲渡側の装置からコンテンツを受信するステップと、を具備することを特徴とする情報処理方法。
【請求項１８】譲渡履歴の各レコードは、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ譲受側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名ＴＳＧを含み、
前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査し、さらにコンテンツが持つ固有情報がコンテンツ送受信間で一致するか否かを検査する、ことを特徴とする請求項１７に記載の情報処理方法。
【請求項１９】前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタＣＡの公開鍵P_{CA}を用いて暗号化したもので置換する、ことを特徴とする請求項１８に記載の情報処理方法。
【請求項２０】複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する情報処理方法であって、
前記譲渡履歴は、
コンテンツ固有の情報ＴＩＤと、
コンテンツを譲渡する度に追加されるレコードと、
を含み、
コンテンツ及び譲渡履歴を受信するステップと、
譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする情報処理方法。
【請求項２１】前記不正検出ステップでは、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信したことに応答して、不正の検出を開始する、ことを特徴とする請求項２０に記載の情報処理方法。
【請求項２２】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、
前記不正検出ステップでは、譲渡履歴の各レコードに含まれるＳＩＤがコンテンツを発行する所定の装置を示していない場合には、該ＳＩＤによって識別される装置を不正者として特定する、ことを特徴とする請求項２０に記載の情報処理方法。
【請求項２３】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、
前記不正検出ステップでは、譲渡履歴の先頭レコードに含まれるＳＩＤがコンテンツを発行する所定の装置を示していない場合には、該ＳＩＤによって識別される装置を不正者として特定する、ことを特徴とする請求項２０に記載の情報処理方法。
【請求項２４】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含み、
前記不正検出ステップでは、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信した場合には、各コンテンツが持つ譲渡履歴を比較して、同じコンテンツ固有情報ＴＩＤを持つコンテンツに付随する譲渡履歴が正しく先頭のコンテンツ送信側の装置固有情報ＳＩＤのレコードから始まり且つ途中まで同一内容のレコードを持つが異なり始める枝分かれするレコードを探索し、該枝分かれしたレコード中のコンテンツ送信側の装置固有情報ＳＩＤによって識別される装置を不正者として特定する、ことを特徴とする請求項２０に記載の情報処理方

法。

【請求項２５】前記不正検出ステップでは、

譲渡履歴の各レコードが所定の管理センタＣＡの公開鍵P_{CA}で暗号化されている場合には、譲渡履歴に含まれる各レコードを最新のものから順に該管理センタＣＡの秘密鍵S_{CA}によって復号化して検査し、

正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを特徴とする請求項２０に記載の情報処理方法。

【請求項２６】他の装置にコンテンツを譲渡する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ ソフトウェアは、

コンテンツ譲受側の装置と相互認証するステップと、

コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ受信側が発生したノンスＴＮ、並びにコンテンツの譲渡履歴全体に対する電子署名ＴＳＧを含んだ新規レコードを追加してコンテンツの譲渡履歴を更新するステップと、

コンテンツの譲渡履歴をコンテンツ譲受側の装置に送信するステップと、

前記相互認証並びにコンテンツ譲受側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲受側の装置に送信するステップと、を具備することを特徴とする記憶媒体。

【請求項２７】他の装置からコンテンツを譲受する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ ソフトウェアは、

コンテンツ譲渡側の装置と相互認証するステップと、

コンテンツ譲渡側の装置にノンスＴＮを送信するステップと、

コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ譲受側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名ＴＳＧを含むレコードからなるコンテンツの譲渡履歴をコンテンツの譲渡側の装置から受信するステップと、

譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査するステップと、

コンテンツ譲渡側の装置からコンテンツを受信するステップと、を具備することを特徴とする記憶媒体。

【請求項２８】前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタＣＡの公開鍵P_{CA}を用いて暗号化したものを置換する、ことを請求項２７に記載の特徴とする記憶媒体。

【請求項２９】複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、

前記譲渡履歴は、

コンテンツ固有の情報ＴＩＤと、

コンテンツを譲渡する度に追加されるレコードと、を含み、

前記コンピュータ ソフトウェアは、

コンテンツ及び譲渡履歴を受信するステップと、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信したことに応答して、譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする記憶媒体。

【請求項３０】前記不正検出ステップでは、

譲渡履歴の各レコードが所定の管理センタＣＡの公開鍵P_{CA}で暗号化されている場合には、譲渡履歴に含まれる各レコードを最新のものから順に該管理センタＣＡの秘密鍵S_{CA}によって復号化して検査し、

正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定する、ことを請求項２９に記載の特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、乗車券、入場券、会員所、許可書、サービス券などの電子チケットを始めとする各種のデジタル情報を不正利用から保護する情報処理装置及び方法、並びに記憶媒体に係り、特に、デジタル情報を耐久性のあるハードウェア上に保持することによって複数の機器間でデジタル情報の譲渡を繰り返す過程において不正利用から保護する情報処理装置及び方法、並びに記憶媒体に関する。

【０００２】更に詳しくは、本発明は、デジタル情報を複数の機器間で譲渡を繰り返す過程において万一ある機器ハードウェアが解析・改変された場合であってもデジタル情報を不正利用から保護する情報処理装置及び方法、並びに記憶媒体に係り、特に、ハードウェアの解析・改変によるデジタル情報の不正利用を検出することによってハードウェアの解析・改変への潜在的な意図を抑制する情報処理装置及び方法、並びに記憶媒体に関する。

【０００３】

【従来の技術】昨今の情報処理、情報通信技術の急速な

進歩に伴い、あらゆる情報がデジタル化されてコンピュータ上で取り扱うことができるようになり、さらには、コンピュータ・ネットワークやメディアを媒介として複数のシステム間で情報が共有・流通されるようになってきている。また、インターネットの爆発的な普及に伴い、デジタル情報を即時的に配信・配布することが可能となっている。すなわち、遠い距離離れた場所に存在する情報資源であっても、それがデジタル化すなわちコンピュータライズされてさえいれば、何処からでも容易且つ瞬時に取得することができる。例えば、映像や音楽などのコンテンツや、コンサートのチケットなどはデジタル化され、ネットワーク上で流通・販売されている。いまやデジタル情報は、それ自体が経済価値のある取引の対象なのである。

【０００４】しかしながら、情報の伝達と共有の容易性というデジタル情報本来の利点も、その応用範囲の拡大によって、新たな問題が発生してきている。何故ならば、デジタル形式の情報の複製や改竄は極めて容易であり、さまざまな不正行為による危険に無防備にさらされるからである。とりわけ、ソフトウェアや音楽情報などの著作権によって保護されるべき情報や、証明書や有価証券など唯一性が重要な情報に関しては、著作権法やその他の情報の複製・改竄に関する法規制を強化するだけでは不充分であり、情報技術の観点からも保護を拡充する必要があると思料される。

【０００５】従来であれば、例えば音楽情報はＣＤやレコードなどのメディアに記録して流通・販売されていた。これら記録メディアからの完全な複製は技術的に困難であるため、複製利用が大きな問題とはなりえなかった。しかしながら、近年、情報を複製するツールでもあるパーソナル・コンピュータ（ＰＣ）や周辺機器が発達し一般消費者でも安価に入手できることができるようになってきたため、それら記録メディアから完全な形態でデジタル情報を抽出することができ、扱い易く加工することを容易になってしまった。また、このようにして得られた音楽情報が、ネットワークを通じて不特定多数に不正に配信されてしまうという状況が生じている。このことは、音楽などコンテンツの制作者又はその著作権者や、これら情報コンテンツを商品としてきた産業界に大きな脅威を与える。情報コンテンツの不正利用の横行を許容すれば、音楽等のコンテンツ制作者やソフトウェア開発者は新たな創作意欲を喪失し、産業活動自体が沈滞してしまいかねない。

【０００６】一方、乗車券、入場券、会員所、許可書、サービス券などの証明書や有価証券は、いままでは、容易に複製・偽造されないように特殊な加工（例えば、透かしや特殊印刷や模様、検印など）が施された紙やその他の媒体を用いて、その上に証明書や有価証券としての情報を記録していた。証明書や有価証券としての情報自体が複製されても、それを記録した媒体である紙が存在しなければ（すなわち特殊加工が検出されなければ）、情報の効力を持たなくすることによって、証明書や有価証券が表す価値の複製を防いできた。

【０００７】この種の証明書や有価証券に関しても、デジタル情報化することにより、いわゆる「電子チケット」という形態で、コンピュータ・ネットワーク上で流通・販売することができる。例えば、コンサートのチケットや航空券などは、電話網やコンピュータ・ネットワークを経由して予約することは従来も可能であるが、最終的なチケットの受け取りは郵送や手渡しに委ねられていた。これに対し、電子チケットによれば、予約と購入を同じ手続で済ますことができるので、消費者は店舗に出向く手間が省け、販売者にとってはチケットの流通コストや管理コストなどを削減することができる利益の増大につながる。すなわち、電子チケットによれば、デジタル情報化による伝達の利便性を活かすことができる。しかしながら、電子チケットを普及させるためには、音楽などのデジタル・コンテンツの場合と同様に、デジタル情報の複製や改竄を技術的に確保する必要がある。

【０００８】このため、最近では複製を防ぎながら電子情報を扱うことができるシステムに関して数多の提案がなされている。

【０００９】デジタル情報の保護には、所定の暗号鍵を用いて暗号化したコンテンツを流通・販売するというシステムが一般的であり、既に広汎に採用されている。例えば、暗号鍵の販売という形式で情報の利用に対して課金を行うことができる。但し、暗号鍵の流通・配布のため、暗号鍵自体もデジタル化してしまうことが多い。このような場合、コンテンツやチケットなど本来の流通・販売の対象である情報と同様に、暗号鍵も複製や改竄が容易となってしまうので、これを技術的に保護しなければならない。

【００１０】例えば、本出願人に既に譲渡されている特開平１１－３２８８５０号公報には、コンテンツの保護を充分図るとともに正当な課金を行うことができる情報配信システムについて開示されている。同公報によれば、コンテンツ・サーバには、Ｃキーにより暗号化されたコンテンツとＣキーとが蓄積されるコンテンツ・データベースが設けられている。このＣキーにより暗号化されたコンテンツとＣキーをＭキーで暗号化して、ユーザ・マシンに送る。ユーザ・マシン上では、Ｃキーにより暗号化されたコンテンツとＣキーをストレージ・デバイスに保存する。そして、再生時にストレージ・デバイスからのＣキーにより暗号化されたコンテンツとＣキーを暗号化／復号化処理チップに送出して復号するとともに、Ｃキーに応じて課金を行う。また、Ｃキーには、時間の経過とともに動的に変化するＤＡコードを付加しておく。このようなＤＡコードを付加することで、Ｃキーを退避させておいて、コンテンツを不正利用するようなことが防止できるとともに、ＤＡコードを利用して、コ

ンテンツの使用期間に制限を持たせたり、所定期間コンテンツを貸借することができる。

【0011】同公報では、比較的大きな電子情報を扱う方法が示されているため、電子情報は複製や改竄されないように暗号化されてハード・ディスクなどの一般の記憶装置に保持される。但し、暗号化の鍵は保持装置のハードウェアに組み込まれているので、読み出すことができない。したがって、保持されている電子情報を読み出しても、電子情報を復号化して用いることはできない。電子情報を使うときには、ハードウェアの回路内でだけ復号化して利用され、外部には復号化された電子情報は漏れないようになっている。ハードウェアで保護したい電子情報の利用を制限し、それによって複製されることを防いでいる。

【0012】また、ICカードを用いたようなセキュリティ システムの場合には、ICカード間で鍵を配布・交換することによって、情報のセキュリティをハードウェア的に維持するようになっている。ICカードに内蔵された電子情報が勝手に読み書きできない（又は耐タンパ性を備えた）半導体メモリ上に鍵などの情報が保持され、認証鍵を知るものだけが読み書きできる。そのため認証鍵を利用するものが、ICカード上の電子情報を複製することなく移動することを注意深く行うことにより、電子情報をICカード間でやり取りしつつ、その複製を防ぐことができる。例えば、別のICカードに情報を移動させたときには、必ず元のICカードの内容を削除するようにする（通常ハードウェアで実現する）。

【0013】また、ソニー株式会社が提供するシステム"MagicGate Memory Stick"では、ICカードに類似した仕組みによる情報セキュリティを実用化している。このMagicGateでは、まずICカード相互間で認証した後に、一方の装置から他方の装置に鍵を明け渡し、最後に元の装置から鍵を消去するようになっている。こうしたシステムでは、デジタル情報としての移動の容易性を依然として維持しつつ、複製や改竄の容易さという性質の制限を実現することができる。

【0014】ICカードなどの特定のハードウェアを用いてデジタル情報を保護するシステムにおいては、ハードウェアの解析・改変に対する耐久性（耐タンパ性）が確保されていることが重要な前提となる。上述したように、デジタル情報を複製、改竄されないように保持する仕組みは大きな利点があり、今後とも活用されていく技術であると考えられるので、ハードウェアの耐久性が破られないように解析・改変がより困難なハードウェアを開発し採用する必要がある。

【0015】しかしながら、ハードウェアは人工物であり、完全とは言い難い。すなわち、コストをいとはわければ（あるいは、鍵を破ることにより得られるデジタル情報にコストを回収するだけの経済的価値が見出されるならば）、鍵を破ることは不可能ではない。このため、単にハードウェアの耐久性を向上させるだけではなく、万一解析・改変された場合にはそれが検出できること、さらにはその結果の不正による被害を食い止められることが重要となる。

【0016】特に、ハードウェアの耐久性を充分に高めた場合、それに対する解析・改変は計画的、組織的なものとならざるを得ない。この場合にも、解析・改変を行うか否かは、その結果として可能になる情報の不正利用によってコストを回収できるか（すなわち情報の経済的価値）が重要になる。したがって、解析・改変によって可能となる不正が容易に検出され不正者を特定できるということは、言い換えればこうした情報の不正利用のやり逃げを困難なものにし、結果としてハードウェアの解析・改変への潜在的な意図を抑制するのに非常に効果的であると思料される。

【0017】

【発明が解決しようとする課題】本発明は、上述したような技術的課題を鑑みたものであり、ハードウェアの不正解析がなされ、その結果として複製されないように保持されていたデジタル情報の複製が可能になり、それが比較的大規模に流通した場合に、そのことが検出でき、さらにどのハードウェアが不正解析されたかが特定できる仕組みを提案することを目的とする。

【0018】その仕組みは、最初に個々のコンテンツに唯一性を持たせて流通させ、後にコンテンツを回収した際に、複数の同一コンテンツが発見された場合には、流通の過程でコンテンツの複製が行われたことが判ることである。さらに、それぞれのコンテンツに譲渡履歴を付随させて、複数の保持装置への譲渡がどの時点で発生したかを調べることができることである。

【0019】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、装置間でコンテンツを交換する情報処理装置であって、コンテンツ及びコンテンツの譲渡履歴を送信及び／又は受信する通信手段と、装置固有の情報を保管する固有情報保持手段と、コンテンツを交換する相手側の装置と相互認証する認証手段と、コンテンツを保持するコンテンツ保持手段と、コンテンツの譲渡履歴を管理する譲渡履歴管理手段と、を具備することを特徴とする情報処理装置である。

【0020】ここで、前記認証手段は、例えば、コンテンツを交換する相手側の装置との間で互いの電子署名を用いた認証を行うことができる。

【0021】また、前記譲渡履歴管理手段は、コンテンツ受信時にはノンスTNを発生し、コンテンツ送信時には、コンテンツ送信側の装置固有情報SID、コンテンツ受信側の装置固有情報RID、コンテンツ受信側が発生したノンスTN、並びにコンテンツの譲渡履歴全体に対する電子署名TSGを含んだ新規レコードをコンテン

ツの譲渡履歴に追加するようにして、コンテンツの移動に関する記録である譲渡履歴をとるようにする。

【0022】したがって、前記譲渡履歴管理手段は、コンテンツ受信時に、コンテンツに付随する譲渡履歴の最後のレコードにコンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴全体に対するコンテンツ送信側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査することができる。

【0023】また、譲渡履歴を、コンテンツの譲渡履歴全体に対する電子署名ＴＳＧをレコードに含めるという一種の「入れ子構造」とすることにより、それぞれのコンテンツ交換時に必要な譲渡履歴検査のために必要な計算のうち、計算処理量の大きい公開鍵暗号の処理回数が譲渡回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による譲渡履歴の改竄に対する耐久性をも実現することができる。

【0024】また、前記譲渡履歴管理手段は、コンテンツ送信側から受信側に以前のコンテンツ譲渡に対応する暗号化されている譲渡履歴に未だ暗号化されていない新規レコードを追加したものを送るようにしてもよい。このような場合、コンテンツ受信側の装置では、未だ暗号化されていない新規レコードを検査した後に、所定の管理センタＣＡ（Certification Authority）の公開鍵P_{CA}を用いて暗号化して、コンテンツの譲渡履歴の未だ暗号化されていない新規レコードを暗号化したものに置き換えるようにしてもよい。このような場合、譲渡履歴を所定のシステム管理者ＣＡ以外には読めないようにすることができるので、システム管理者には不正が行われた情報処理装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどの情報処理装置を経由してきたかを秘密にすることができる。

【0025】前記認証手段によって相手側の装置と相互認証でき、さらに、前記譲渡履歴管理手段によりコンテンツの譲渡履歴の正当性が確認できた場合にのみ、コンテンツの交換を行うようにすることで、正当なコンテンツの流通とコンテンツの保護を確保することができる。この結果、音楽や映像情報などのように経済価値を持つコンテンツや、証明書や有価証券などのように唯一性が重要なコンテンツ（電子チケット）などのデジタル情報を複数の装置にまたがって安全に移動させることができる。

【0026】また、本発明の第２の側面は、複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する情報処理装置であって、前記譲渡履歴は、コンテンツ固有の情報ＴＩＤと、コンテンツを譲渡する度に追加されるレコードと、を含み、前記情報処理装置は、コンテンツ及び譲渡履歴を受信する通信手段と、譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出手段と、を具備することを特徴とする情報処理装置である。

【0027】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、そのレコードより以前に追加されたすべてのレコードを含むコンテンツの譲渡履歴全体に対するコンテンツ送信側の装置による電子署名ＴＳＧを含んでいる。

【0028】したがって、前記不正検出手段は、譲渡履歴に含まれる各レコードの電子署名を最新のレコードから遡りながら検証する。そして、整合しない電子署名のあるレコードを発見した場合には、そのレコードのコンテンツ受信側の装置、すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0029】また、譲渡履歴が所定の所定の管理センタＣＡの公開鍵P_{CA}で暗号化されている場合には、前記不正検出手段は、譲渡履歴に含まれる各レコードを最新のものから順に該管理センタＣＡの秘密鍵S_{CA}によって復号化して検査するようにする。そして、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合には、該レコードを受信した装置すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0030】また、譲渡履歴の先頭レコードに含まれるＳＩＤがコンテンツを発行する所定の装置を示していない場合には、該ＳＩＤによって識別される装置を不正者として特定することができる。

【0031】また、前記不正検出手段は、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信した場合には、各コンテンツが持つ譲渡履歴を比較して、枝分かれレコードを探索する。ここで言う「枝分かれレコード」とは、同じコンテンツ固有情報ＴＩＤを持つコンテンツに付随する譲渡履歴が、正しくコンテンツ発行装置を示す装置固有情報ＳＩＤのレコードから始まり、途中のレコードまで同一のレコードを持ち、あるレコードから異なり始める場合に、最初の異なるレコードのことを示す。そして、発見された枝分かれレコード中のコンテンツ送信側の装置固有情報ＳＩＤによって識別される装置を不正者として特定することができる。

【0032】また、本発明の第３の側面は、他の装置にコンテンツを譲渡する情報処理方法であって、コンテンツ譲受側の装置と相互認証するステップと、コンテンツの譲渡履歴を更新するステップと、コンテンツの譲渡履歴をコンテンツ譲受側の装置に送信するステップと、前記相互認証並びにコンテンツ譲受側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲受側の装置に送

信するステップと、を具備することを特徴とする情報処理方法である。

【００３３】前記のコンテンツの譲渡履歴を更新するステップでは、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ受信側が発生したノンスＴＮ、並びにコンテンツの譲渡履歴全体に対する電子署名ＴＳＧを含んだ新規レコードをコンテンツの譲渡履歴に追加する。

【００３４】したがって、コンテンツ譲受時において、コンテンツに付随する譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴全体に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査することができる。

【００３５】また、譲渡履歴をコンテンツの譲渡履歴全体に対する電子署名ＴＳＧをレコードに含めるという一種の入れ子構造とすることにより、それぞれのコンテンツ交換時に必要な譲渡履歴検査のために必要な計算のうち、計算処理量の大きい公開鍵暗号の処理回数が譲渡回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による譲渡履歴の改竄に対する耐久性をも実現することができる。

【００３６】前記のコンテンツの譲渡履歴を更新するステップでは、コンテンツ送信側から受信側に、これまでのコンテンツ譲渡に対応する暗号化された譲渡履歴に未だ暗号化されていない新規レコードを追加したものを送る。これに対し、コンテンツ受信側では、新規レコードを検査した後、それを所定の管理センタＣＡの公開鍵P_{CA}を用いて暗号化した後に、コンテンツの譲渡履歴の未だ暗号化されていない新規レコードを暗号化したもので置換するようにしてもよい。このような場合、譲渡履歴を所定のシステム管理者以外には読めないようにすることができるので、システム管理者には不正が行われた情報処理装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどの情報処理装置を経由してきたかを秘密にすることができる。

【００３７】また、本発明の第４の側面は、他の装置からコンテンツを譲受する情報処理方法であって、コンテンツ譲渡側の装置と相互認証するステップと、コンテンツ譲渡側の装置にノンスＴＮを送信するステップと、コンテンツの譲渡側の装置からコンテンツの譲渡履歴を受信するステップと、受信した譲渡履歴を検査するステップと、コンテンツ譲渡側の装置からコンテンツを受信するステップと、を具備することを特徴とする情報処理方法である。

【００３８】譲渡履歴の各レコードは、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ譲受側の装置が発生したノンスＴＮ、並びに、そのレコードよりも以前に追加されたすべてのレコードを含むコンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名ＴＳＧを含んでいる。

【００３９】したがって、前記の譲渡履歴を検査するステップでは、譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴全体に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査し、コンテンツの流通過程における不正行為のあったコンテンツの受け取りを拒否する。

【００４０】また、譲渡履歴はコンテンツの譲渡履歴全体に対する電子署名ＴＳＧをレコードに含めるという一種の入れ子構造となっているので、それぞれのコンテンツ交換時に必要な譲渡履歴検査のために必要な計算のうち、計算処理量の大きい公開鍵暗号の処理回数が譲渡回数によらない一定値となるので、全体の計算時間が短縮される。併せて、コンテンツ流通の途中で不正者による譲渡履歴の改竄に対する耐久性を実現することができる。

【００４１】コンテンツの譲渡履歴が暗号化されている場合、コンテンツの譲渡側から、それ以前の譲渡に対応するすべてのレコードを暗号化したものからなる譲渡履歴に、今回の譲渡に対応する未だ暗号化されていない新規レコードが追加されたものを受け取る。コンテンツ譲受側では、この新規レコードを検査して、該レコードが正しい場合には、それを所定の管理センタＣＡの公開鍵P_{CA}で暗号化する。そして、譲渡履歴の暗号化されていない新規レコードをこの暗号化したもので置換する。これにより、ＣＡなどのシステム管理者以外がコンテンツの流通経路の秘密を知り得るということを防止することができる。

【００４２】また、本発明の第５の側面は、複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する情報処理方法であって、前記譲渡履歴は、コンテンツ固有の情報ＴＩＤと、コンテンツを譲渡する度に追加されるレコードと、を含み、コンテンツ及び譲渡履歴を受信するステップと、譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする情報処理方法である。

【００４３】譲渡履歴の各レコードは、コンテンツ送信側の装置固有情報ＳＩＤ、コンテンツ受信側の装置固有情報ＲＩＤ、コンテンツ受信側の装置が発生したノンスＴＮ、並びに、そのレコードよりも以前に追加されたすべてのレコードからなるコンテンツの譲渡履歴に対するコンテンツ送信側の装置による電子署名ＴＳＧを含んでいる。

【0044】したがって、前記不正検出ステップでは、譲渡履歴に含まれる各レコードの電子署名を最新のレコードから遡りながら検証して、整合しない電子署名をしたコンテンツ送信側の装置を不正者として特定することができる。

【0045】また、譲渡履歴が所定の所定の管理センタCAの公開鍵P_{CA}で暗号化されている場合には、前記不正検出ステップでは、譲渡履歴に含まれる各レコードを最新のものから順に譲渡管理センタCAの秘密鍵S_{CA}によって復号化して検査するようにする。そして、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合には、該レコードを受信した装置すなわちそのレコードの次のレコードの送信側の装置を不正者として特定することができる。

【0046】また、前記不正検出ステップでは、譲渡履歴の先頭レコードに含まれるＳＩＤがコンテンツを発行する所定の装置を示していない場合には、該ＳＩＤによって識別される装置を不正者として特定することができる。

【0047】また、前記不正検出ステップでは、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信した場合には、各コンテンツが持つ譲渡履歴を比較して、枝分かれするレコードを探索する。ここで言う「枝分かれレコード」とは、同じコンテンツ固有情報ＴＩＤを持つコンテンツに付随する譲渡履歴が、正しくコンテンツ発行装置を示す装置固有情報ＳＩＤのレコードから始まり、途中のレコードまで同一のレコードを持ち、あるレコードから異なり始める場合に、最初の異なるレコードのことを示す。そして、発見された枝分かれレコード中のコンテンツ送信側の装置固有情報ＳＩＤによって識別される装置を不正者として特定することができる。

【0048】しかして、本発明に係る情報処理装置又は方法によれば、最初に個々のコンテンツに唯一性を持たせて流通させ、後にコンテンツを回収した際に、複数の同一コンテンツが発見された場合には、流通の過程でコンテンツの複製が行われたことが判る。さらに、それぞれのコンテンツに譲渡履歴を付随させて、複数の保持装置への譲渡がどの時点で発生したかを調べることができる。

【0049】これに類似する技術は、譲渡可能な電子現金の方法の一部として既に提案されている。例えば、T. Okamoto et al著の“Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash”（Advances in Cryptology Cryto'89, Lecture Notes in Computer Science 435, pp.481-496, Springer-Verlag, Berlin (1989)）や、日本国特許第２０２７７１３号「電子現金実施方法及びその装置」、D. Chaum及びT. P. Pedersen著の“Transferred Cash Grows in Size”（Advances in Cryptology Eurocrypt'92, LectureNotes in Computer Science, pp. 390-407, Springer-Verlag, Berlin (1992)）などでは、電子現金に関する手法が記述されている。これらの電子現金の場合には、デジタル情報として表される現金が多重に支払われることを阻止する方法が採用されている。しかし、これらの文献に記載された方法では、コンテンツなかも電子現金の譲渡の際に、付随する譲渡履歴のすべての検査を行う必要がある。つまり、譲渡の回数に比例した計算量が必要であり、譲渡回数が増えた場合に、計算量が膨大になるという欠点がある。また、これら上述の文献はいずれも、電子現金という使用目的に特化した方法であり、音楽コンテンツなどの一般のコンテンツ流通に適用することは難しい。

【0050】これに対し、本発明に係る情報処理装置及び方法では、譲渡履歴のデータ構造を入れ子構造とすることで、各譲渡時に必要な譲渡履歴検査のための計算量を譲渡回数に依存しない一定値としながら、流通途中での不正者による譲渡履歴の改竄に対する耐久性をも実現することができる。

【0051】例えば、個々のコンテンツ毎に区別がつき、不正がない限りシステム内にそれぞれが唯一存在し、一定期間の後に回収されるような条件を満たすコンテンツに対しては、本発明を容易に適用することができる。

【0052】また、本発明の第６の側面は、他の装置にコンテンツを譲渡する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ ソフトウェアは、コンテンツ譲受側の装置と相互認証するステップと、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ受信側が発生したノンスＴＮ、並びにコンテンツの譲渡履歴全体に対する電子署名ＴＳＧを含んだ新規レコードを追加してコンテンツの譲渡履歴を更新するステップと、コンテンツの譲渡履歴をコンテンツ譲受側の装置に送信するステップと、前記相互認証並びにコンテンツ譲受側の装置からの譲渡履歴の確認後にコンテンツをコンテンツ譲受側の装置に送信するステップと、を具備することを特徴とする記憶媒体である。

【0053】また、本発明の第７の側面は、他の装置からコンテンツを譲受する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ ソフトウェアは、コンテンツ譲渡側の装置と相互認証するステップと、コンテンツ譲渡側の装置にノンスＴＮを送信するステップと、コンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、コンテンツ譲受側の装置が発生したノンスＴＮ、並びに、コンテンツの譲渡履歴全体に対するコンテンツ譲受側の装置による電子署名ＴＳＧを含むレコードからなるコンテンツの譲渡履歴をコンテンツの

譲渡側の装置から受信するステップと、譲渡履歴の最後のレコードにコンテンツ譲渡側の装置固有情報ＳＩＤ、コンテンツ譲受側の装置固有情報ＲＩＤ、自身が生成したノンスＴＮが含まれていること、及び／又は、電子署名ＴＳＧが正しく譲渡履歴に対するコンテンツ譲渡側の装置の署名になっていることを確認することによって、コンテンツの譲渡履歴を検査するステップと、コンテンツ譲渡側の装置からコンテンツを受信するステップと、を具備することを特徴とする記憶媒体である。

【００５４】前記の譲渡履歴を検査するステップでは、コンテンツの譲渡履歴の最後のレコードの検査に成功した場合に、そのレコードを所定の管理センタＣＡの公開鍵P_{CA}を用いて暗号化したもので置換するようにしてもよい。

【００５５】また、本発明の第８の側面は、複数の装置間で譲渡履歴を伴って流通されたコンテンツを回収する処理をコンピュータ上で実行するように記述されたコンピュータ ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記譲渡履歴は、コンテンツ固有の情報ＴＩＤと、コンテンツを譲渡する度に追加されるレコードと、を含み、前記コンピュータ ソフトウェアは、コンテンツ及び譲渡履歴を受信するステップと、同じコンテンツ固有情報ＴＩＤを持つコンテンツを２回以上受信したことに応答して、譲渡履歴を検査してコンテンツの流通過程における不正を検出する不正検出ステップと、を具備することを特徴とする記憶媒体である。

【００５６】前記不正検出ステップでは、譲渡履歴の各レコードが所定の管理センタＣＡの公開鍵P_{CA}で暗号化されている場合には、譲渡履歴に含まれる各レコードを最新のものから順に該管理センタＣＡの秘密鍵S_{CA}によって復号化して検査して、正しく復号化できない、あるいは署名を正しく検証できないレコードを検出した場合に、該レコードを受信した装置を不正者として特定するようにしてもよい。

【００５７】本発明の第６乃至第８の各側面に係る記憶媒体は、例えば、様々なプログラム コードを実行可能な汎用コンピュータ システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disk）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【００５８】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第６乃至第８の各側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアを所定のコンピュータ上にインストールすることによって、該コンピュータ上では協働的作用が発揮され、本発明の第３乃至第５の各側面に係る情報処理方法と同様の作用効果を得ることができる。

【００５９】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００６０】

【発明の実施の形態】本発明の実施形態について記述する前に、まず、本発明において用いられる暗号技術上の幾つかの用語について説明する。

【００６１】共通鍵暗号

本発明では、「共通鍵暗号」と呼ばれるアルゴリズムと、「公開鍵暗号」、「電子署名」と呼ばれるアルゴリズムを利用する。共通鍵暗号は「対称暗号」とも呼ばれ、データを暗号化する際に用いる鍵と復号化する際に用いる鍵が同じ、あるいは異なる場合でも一方から他方を算出することが容易であるという性質を持った暗号アルゴリズムである。代表的な共通鍵暗号アルゴリズムとしては、アメリカ合衆国商務省標準局が標準暗号として認定した"ＤＥＳ（data encryption standard）"や"Ｔｒｉｐｐｌｅ ＤＥＳ"、ＮＴＴの"ＦＥＡＬ（fast data enciphermentalgorithm）"などを挙げることができる。以下では、共通鍵Ｋによりｍを暗号化して、暗号文ｃを得る場合をｃ＝Ｅ（ｋ，ｍ）と表現し、また、その復号化をｍ'＝Ｄ（Ｋ'，ｃ）と表現することにする。この場合、ＫとＫ'が一致すれば、ｍとｍ'も一致することとする。

【００６２】公開鍵暗号

公開鍵暗号は「非対称暗号」とも呼ばれ、データを暗号化する際に用いる鍵と、復号化する際に用いる鍵が異なり、且つ、一方から他方を算出することが非常に困難であるという性質を持った暗号アルゴリズムである。この公開鍵暗号アルゴリズムによれば、一方の鍵で暗号化した情報は、他方の鍵でしか復号化することができない。暗号化の鍵は「公開鍵」と呼ばれ、一般に公開して誰でも使用できるようにする。また、復号化の鍵は「秘密鍵」と呼ばれ、他人に漏れないように所有者が管理する。これによって、任意の送り手は公開鍵で暗号化することによって、秘密鍵を所持する受け手にしか復号化することができない暗号文を送信することができる。公開鍵をP_k、秘密鍵をS_kとしたとき、公開鍵P_kによりデータＭを暗号化することをＣ＝Ｅ（P_k，Ｍ）と表現し、また、秘密鍵S_kにより暗号文Ｃを復号化することをＭ＝Ｄ（S_k，Ｃ）と表現する。重要な性質は、秘密鍵S_kを秘密に保てば、公開鍵P_kや暗号文Ｃが知られたとしても、元の平分Ｍが得られないという点である。公開鍵暗号アルゴリズムとしては、"ＲＳＡ（Rivest Sham

ir Adleman ）”暗号や、楕円曲線暗号などが知られている。

【００６３】電子署名

電子署名は、データ通信における印鑑やサインに相当する機能であり、受け取った情報が確かに送り手が送ったものであることを保証したり（偽造防止）、受け手が受け取った情報の内容を勝手に書き替えたり、その内容が送られてきた内容だと言い張れないようにする（改竄防止）、などの目的で使用される。例えば、上述した公開鍵暗号アルゴリズムを応用することによって、電子署名を実現することができる。ここでは、ＲＳＡ署名の場合を念頭に上で用いた公開鍵暗号の記法を用いて説明する。データＭが存在するとき、Ｍの作成者が自分の秘密鍵S_kを用いて、電子署名ＳＧ（Ｍ）＝Ｄ（S_k，ｈ（Ｍ））を計算する。ここで、ｈ（ ）は一方向性関数であり、出力値から入力値を知る（又は現像する）ことが非常に困難だという性質を持つ。こうした関数としては“ＭＤ５（message digest algorithm 5）”や“ＳＨＡ－１（secure hash algorithm 1）”と呼ばれるものが挙げられる。データＭを送る際に（Ｍ，ＳＧ（Ｍ））の組で送ると、受け取り側は、ｈ（Ｍ）＝Ｅ（P_k，ＳＧ（Ｍ））が満たされるかどうかを確認することで、Ｍが改竄されていないことと、電子署名ＳＧ（Ｍ）が秘密鍵S_kの所有者によって付加されたものであることを確認することができる。すなわち、メッセージ作成者が自分の秘密鍵でメッセージを暗号化することにより、暗号化メッセージの受け取り手は作成者の公開鍵でしか復号化できないので、メッセージすなわち署名の偽造や改竄ができない。以下、このような手続きのことを「署名確認」と呼ぶ。電子署名としては、ＲＳＡ署名やＥＩＧａｍａｌ署名、楕円ＥｌＧａｍａｌ署名などが挙げられる。電子暗号との混乱を避けるために、署名生成に使う秘密鍵S_kのことを「署名生成鍵」と呼び、署名検証に使う公開鍵P_kのことを「署名検証鍵」と呼ぶ。また、署名生成鍵、署名検証鍵と記述する場合には、署名で使用される一方向性関数を特定する情報も含まれているものとする。

【００６４】チャレンジ＆レスポンス認証

チャレンジ・コードと呼ばれる１回限りの数字（タイムスタンプや乱数など）を基に認証を安全に実施する手法である。公開鍵暗号アルゴリズムを応用することにより、チャレンジ＆レスポンス認証を実現することができる。公開鍵P_kを使って、相手が秘密鍵S_kを所有することを、秘密鍵自体を知ることなく確認することができる。例えば、検証側で乱数ｒを生成し、ｒ’＝Ｅ（P_k，ｒ）を計算して相手に送る。これに対し、相手が正しく元の乱数ｒ＝Ｄ（S_k，ｒ’）を計算して検証側に返すことによって、検証側では相手がS_kを所有していることを確認できる。あるいは、検証側から乱数ｒを相手に送り、相手がｒ”＝Ｄ（S_k，ｈ（ｒ））を計算して返す。これに対し、検証側では、ｈ（ｒ）＝Ｅ（P_k，ｒ”）が成り立てば、相手は秘密鍵S_kを所有していることが確認される。同様に電子署名の手法により、署名検証鍵P_kを使って、相手が署名生成鍵S_kを所有することを、署名生成鍵自体を知ることなく確認することができる。すなわち、検証側から乱数ｒを生成し相手に送る。これに対し、相手はＳＧ（ｒ）＝Ｄ（S_k，ｈ（ｒ））を計算して返送する。そして、検証側では、ｈ（ｒ）＝Ｅ（P_k，ＳＧ（ｒ））が成立すれば、相手が署名生成鍵S_kを所有していることが確かめられる。チャレンジ＆レスポンス認証により、特定の秘密鍵あるいは署名生成鍵が存在することを、対応する公開鍵あるいは署名検証鍵を用いて、秘密鍵あるいは署名生成鍵自体を知ることなく確認することが可能である。

【００６５】証明書

特定の相手を認証する（あるいは、特定の相手だけに情報を伝える、特定の相手が作成した文書であることを確認する）ためには、相手が所有する秘密鍵に対応する公開鍵、あるいは署名生成鍵に対応する署名検証鍵を正しく把握していることが重要である。しかし、そうした相手が多い場合には、すべてを把握しておくことは困難である。このために、１つだけ正しい署名検証鍵を把握していれば、それを基にして、他の公開鍵あるいは署名検証鍵を連鎖的に正しく把握する方法が提案されている（ＩＴＵ－ＴのＸ．５０９勧告）。１つだけ把握すべき署名検証鍵に対応する署名生成鍵の所有者のことを、一般に「認証センター（ＣＡ：Certification Authority）」と呼ぶ。ＣＡは、公開鍵が間違いなく所有者本人のものであることを証明可能な第３者機関であり、公正且つ中立な立場にあり、絶対的に信頼できるものであることを前提とする。ＣＡは、ＣＡ自身の秘密鍵で暗号化した証明書を発行する。すなわち、証明書はＣＡの電子署名が付加されているので、他人が勝手に偽造することができない。ＣＡの署名検証鍵 生成鍵の組を（P_{CA}，S_{CA}）とし、署名検証鍵P_{CA}が公開されシステムの参加装置に正しく伝えられている署名検証鍵であるとする。また、署名生成鍵S_{CA}は、チケット・システム管理センターだけが使用できるとする。それ以外の公開鍵あるいは署名検証鍵P_nに関しては、その所有者と結びつく情報Ｉｎｆｏ$_n$とP_nを組にしたもの（Ｉｎｆｏ$_n$，P_n）に、ＣＡが署名生成鍵S_{CA}を使って生成した署名SG_n＝Ｄ（S_{CA}，ｈ（Ｉｎｆｏ$_n$，P_n））を付加した証明書（Ｉｎｆｏ$_n$，P_n，SG_n）を発行する。これによって、ＣＡが Ｉｎｆｏ$_n$で特定される所有者とP_nの関係を保証したことになる。

【００６６】証明書検証

証明書を利用する際には、秘密鍵又は署名生成鍵S_nの所有者は、最初に証明書（Ｉｎｆｏ$_n$，P_n，SG_n）を署名検証鍵に示す。検証側は、ＣＡの公開鍵P_{CA}を用いて証明書の署名確認を行うことによって（ｈ（Ｉｎｆｏ

$_n$，P_n）＝E（P_{CA}，SG_n））、証明書の正当性を検証する。この結果、$Info_n$の示す内容がP_nで認証できる（公開鍵P_nに対応する秘密鍵S_nを持つ、又は、署名検証鍵P_nに対応する署名生成鍵S_nを持つ）相手と結びつくことを確認することができる。例えば、$Info_n$が人名であれば、P_nで認証できる相手の人名が判明する。証明書には、一般には、暗号のアルゴリズムや、使用されている一方向性関数の種類の情報も含まれる。以下の説明で証明書について区別が必要である場合、電子署名の検証鍵に関するものである場合は「署名証明書」と呼び、公開鍵暗号の公開鍵に関するものである場合には「鍵証明書」と呼ぶことにする。また、証明書の情報$Info_n$で伝えられるべき内容がない場合であっても、P_nで認証できる相手がCAに登録されていることを確認する目的で、証明書検証アルゴリズムが用いられる場合もある。

【００６７】なお、本発明の要旨は、特定の暗号アルゴリズムに依存するものではない。以下の説明では、暗号アルゴリズムの一般的性質のみを用いて考案されている。したがって、説明中でも暗号の種類（共通鍵暗号、公開鍵暗号、電子署名）だけを記すことにする。

【００６８】本発明は、ハードウェア構精を利用して、コンテンツを複製されないように流通させることのできるシステムに関するものである。本発明によれば、ＩＣカードなどのシステム中のコンテンツ保持装置のハードウェアが不正に解析又は改変され、本来は唯一性が保たれるべきコンテンツが複製されたとき、同一コンテンツに関わる複数の流通経路から、コンテンツ保持装置に対する不正の有無を検出することができる。本発明によれば、さらに、コンテンツとともに流通する譲渡履歴を利用することにより、どのコンテンツ保持装置で不正が行われたかを特定することができる。

【００６９】本発明に関して、まず適用対象となるシステム、コンテンツ、装置、及びコンテンツ譲渡について説明する。次いで、コンテンツと一緒に流通する譲渡履歴に関して、そのデータ構造、および譲渡履歴を作ったコンテンツ譲渡について説明する。次いで、不正検出のために必要な仮定を説明してから、コンテンツ保持装置に対する不正の有無の検出方法、さらに譲渡履歴を用いて、どのコンテンツ保持装置で不正が行われたかを特定する方法について説明する。そして、本発明によって不正装置の特定が成功することを証明した後、最後に譲渡履歴からコンテンツ流通の情報を収集されることで、コンテンツ流通の匿名性が失われることを防ぐために、譲渡履歴を暗号化する方法について説明する。

【００７０】１．本発明適用のシステム

図１には、本発明の一実施形態に係る、デジタル情報すなわちコンテンツを複製されないように保持するシステム１の構成を模式的に示している。このシステムは、コンテンツ保持装置１０、コンテンツ発行装置３０、コンテンツ回収装置５０の３種類からなる。コンテンツは、コンテンツ発行装置３０で発行され、複数のコンテンツ保持装置１０Ａ，…，１０Ｎ間でやり取りされ、最終的にコンテンツ回収装置５０で回収される。

【００７１】例えば、コンテンツ発行装置３０は、チケットの発券装置に相当する。また、コンテンツ保持装置１０は、ＩＣカードなどチケットを購入した消費者が持ち運ぶ機器に相当する。同図において、複数のコンテンツ保持装置１０Ａ，…，１０Ｎが直列的に並べているのは、コンテンツが各保持装置１０Ａ，…間で順次譲渡されていくこと、すなわちコンテンツの流通を示している。あるコンテンツ保持装置が他のコンテンツ保持装置にコンテンツを成功裏に譲渡したとき、元のコンテンツ保持装置からはコンテンツが消去される。また、コンテンツ回収装置５０は改札などチケットを回収する装置に相当する。必ずしもすべてのコンテンツが回収される訳ではないが、イベントのチケットのように大部分が回収されると仮定する。コンテンツや電子チケットの場合、コンテンツには、その唯一性を示す固有番号が割り当てられ、さらには有効期限が設定されている。

【００７２】本実施形態では、先述した同一システム１に属する各装置、すなわちコンテンツ保持装置１０、コンテンツ発行装置３０、並びにコンテンツ回収装置５０の各々に対して、電子署名の証明書を発行するための管理センタ（ＣＡ）７０が配設されている。その様子を図２に示している。

【００７３】コンテンツ発行装置３０、保持装置１０、回収装置５０は、それぞれに固有の公開鍵P_iと秘密鍵S_iを持つ。管理センタＣＡ７０に公開鍵P_iと装置の固有番号HID_iを登録することで、P_iとHID_iが含まれる署名証明書（$Info_i$，P_i，SG_i）を発行してもらう。

【００７４】ここで、署名証明書（$Info_i$，P_i，SG_i）中の$Info_i$には、対応する装置の固有番号HID_iが含まれるものとする。コンテンツの流通に関わる各装置１０，３０，５０の所有者とHID_iとの対応は、管理センタＣＡ７０だけが把握しているものとする。コンテンツ発行者の署名証明書の場合には、$Info_i$の一部として、コンテンツ発行者か否かが判断できる情報（例えば、チケットの場合であれば買行者名など）が含まれる。各装置１０，３０，５０は、公開鍵P_iと秘密鍵S_i、署名証明書（$Info_i$，P_i，SG_i）を保持する。

【００７５】コンテンツ流通に関わる各装置１０，３０，５０の所有者とHID_iとの対応は、管理センタＣＡ７０だけが把握しているので、特定のHID_iで不正が行われたことが判った場合、管理センタＣＡ７０はその不正行為に関わった装置の所有者を追及することができる。また、各コンテンツに付随する譲渡履歴（後述）によって、あるコンテンツが過去にHID_iに対応する

保持装置10で保持されていたことが判った場合にも、具体的に誰がコンテンツを保持していたかを通常の利用者が知ることはできない。これにより、コンテンツ流通の匿名性が守られる。この点に関しては、後でさらに言及する。

【0076】以下では、説明の便宜上、コンテンツ発行装置30にはIDISSUERが、コンテンツ回収装置50にはIDDEPOSITがそれぞれ割り振られているものとする。また、コンテンツ発行者、コンテンツ回収者、コンテンツ保持者それぞれの署名は、コンテンツ保持装置10、発行装置30、回収装置50において生成される署名のことを指す。コンテンツ回収者は、コンテンツ発行者自身、あるいはその代理人である。

【0077】2．本発明適用のコンテンツ

本実施形態では、ハードウェア機構を利用してコンテンツが複製されないように保持するシステムにおいて、そのハードウェアが不正解析・改変され、コンテンツが複製された場合に、そのことを後から検出し、不正が行われたハードウェアを特定するようになっている。

【0078】但し、本実施形態において取り扱う不正は、コンテンツの複製のみであり、複製以外のコンテンツの改変などは対象としない。したがって、ハードウェアを解析、改変して可能となる不正が、コンテンツの複製のみであるか、あるいはコンテンツの複製のみが摘害や影響の点で重要な場合に有効である。

【0079】さらに、取り扱われるコンテンツが正常に流通している場合には、唯一性があることを仮定する。つまり、このとき同一のコンテンツが存在すれば、ハードウェアの解析・改変によって不正なコンテンツの複製が行われたことになる。そのため、各コンテンツには改竄ができないように固有番号TIDが付けられているとする。そして、各装置間でのコンテンツ受け渡しの度に、コンテンツの固有番号TIDを含めて改竄がないことを検査できるようにする。これを以下では「コンテンツ確認」と呼ぶことにする。

【0080】コンテンツ確認ができる場合としては、例えば、コンテンツに固有の番号TIDと電子署名が付加されているコンテンツ構成が考えられる。図3には、コンテンツの構成例を示している。同図では、コンテンツには、コンテンツを特定する番号TIDと、コンテンツ発行者の署名証明書Certと、電子署名CSGが含まれる。コンテンツ発行者の署名証明書Certは、管理センタCA70により発行され、($Info_i$, P_i, SG_i)で構成される。また、電子署名CSGは、コンテンツ全体（但し、CSG部分は0とする）に対するコンテンツ発行者の電子署名である。コンテンツ本体とTIDとCertとCSG部にあたる0値のビット連結をMとおくと、コンテンツ発行者の電子署名CSG（$=SG_i(M)$）は、$D(S_i, h(M))$で表される。コンテンツ発行者の署名証明書Certによって、電子署名CSGを検証するための鍵が得られるものとする。

【0081】この場合、コンテンツの改竄がないことは、図4にフローチャートの形式で示された処理手順によって確認することができる。以下、このフローチャートに従って、コンテンツの確認処理について説明する。

【0082】まず、署名証明書Certがコンテンツ発行者の署名証明書になっているかを確認する（ステップS1）。

【0083】次いで、管理センタCA70の公開鍵P_{CA}を用いて署名証明書Certの検証を行う（$h(Info_i, P_i) = E(P_{CA}, SG_i)$）（ステップS2）。

【0084】そして、署名証明書Certからコンテンツ発行者の公開鍵P_iを抽出して（ステップS3）、この公開鍵P_iを用いて電子署名CSGを検証する（$h(M) = E(P_i, CSG)$）（ステップS4）。

【0085】図3及び図4に示す例では、コンテンツは、順次明け渡されるコンテンツ保持装置10上で、複製されないようにハードウェア機構で保護される。さらにコンテンツ確認の処理も、不正解析に対する耐久性をもつハードウェアで行われる。コンテンツ譲渡の度に、コンテンツ確認を行うことで、改竄のないコンテンツのみが流通できることになる。

【0086】また、図5には、コンテンツ確認を行うことができる他のコンテンツ構成例を示している。同図に示す例では、各コンテンツは、複製や改竄がなされないように保護されるコンテンツ秘密部と、対応するコンテンツ公開部の組からなる。

【0087】コンテンツ秘密部は、コンテンツ毎に異なる公開鍵暗号の秘密鍵CS_{TID}と付加情報で構成され、対応する公開鍵CP_{TID}を含んだコンテンツ公開部とともに流通する。コンテンツ秘密部は、ICカードなど所定のコンテンツ保持装置10内で外部アクセス不可能な状態で保管される。

【0088】コンテンツ公開部には、公開鍵CP_{TID}、コンテンツを特定する番号TIDと、コンテンツ発行者の署名証明書Certと、電子署名CSGが含まれる。コンテンツ発行者の署名証明書Certは、管理センタCA70により発行され、($Info_i$, P_i, SG_i)で構成される。CSGはコンテンツ公開部全体（但し、CSG部分は0とする）に対するコンテンツ発行者の電子署名である。コンテンツ本体とTIDとCertとCSG部にあたる0値のビット連結をMとおくと、コンテンツ発行者の電子署名CSG（$=SG_i(M)$）は、$D(S_i, h(M))$で表される。コンテンツ発行者の署名証明書Certによって、CSGを検証するための鍵が得られるものとする。コンテンツ公開部は、例えばICカードの外に、外部の装置からアクセス可能な状態に置かれる。

【0089】なお、図5に示すような秘密部と公開部とからなるコンテンツ構成に関しては、本出願人に既に譲

渡されている特願２０００－３７８２６１号明細書（「情報記録媒体、情報処理装置及び情報処理方法、プログラム記憶媒体、並びに情報処理システム」）にも開示されている。

【００９０】異なる公開鍵CP_{ITD}を含むコンテンツ公開部に対応する秘密鍵CS_{ITD}を改竄することは、暗号学的に困難である。また、任意の公開鍵を含むコンテンツ公開部を新たに作成することは、コンテンツ公開部に含まれるコンテンツ発行者の電子署名ＣＳＧによって困難である。これらの帰結として、ハードウェアの解析・改変によって可能になる不正は、付加情報を改変することか、保持しているコンテンツのコンテンツ秘密部を複製することである。付加情報は、チケットに対するはさみの役割をするため、その改変によって可能となるのはチケットの不正な再利用である。本発明の目的は、複製による不正コンテンツの流通を阻止することなので、付加情報の改変による不正は本明細書中では扱わない。以上から、特願２０００－３７８２６１号明細書に開示される「情報記録媒体、情報処理装置及び情報処理方法、プログラム記憶媒体、並びに情報処理システム」の場合も、本発明の適用条件に合う。

【００９１】図５に示したコンテンツに対して改竄がないことは、図６にフローチャートの形式で示した処理手順によって確認することができる。以下、このフローチャートに従って、コンテンツ確認処理について説明する。

【００９２】まず、コンテンツ公開部の確認を行う。すなわち、コンテンツ公開部に含まれる署名証明書Ｃｅｒｔがコンテンツ発行者の署名証明書になっているかを確認し（ステップＳ１１）、次いで、管理センタＣＡ７０の公開鍵P_{CA}を用いて署名証明書Ｃｅｒｔの検証を行う（ｈ（ｉｎｆｏ$_2$，P_2）＝Ｅ（P_{CA}，SG_2））（ステップＳ１２）。

【００９３】次いで、署名証明書Ｃｅｒｔからコンテンツ発行者の公開鍵P_2を抽出して（ステップＳ１３）、この公開鍵P_2を用いて電子署名ＣＳＧを検証する（ｈ（Ｍ）＝Ｅ（P_2，ＣＳＧ））（ステップＳ１４）。

【００９４】ステップＳ１１～Ｓ１４では、コンテンツ公開部の正当性を確認した。次いで、ステップＳ１５以降では、コンテンツ秘密部側の正当性の確認を行う。本実施形態では、確認したコンテンツ公開部から公開鍵CP_{ITD}を取り出し、これを使って対応するコンテンツ秘密部（秘密鍵CS_{ITD}）が存在するかをチャレンジ・レスポンス認証によってコンテンツ秘密部の正当性を確認する。

【００９５】チャレンジ・レスポンス認証では、まず、コンテンツ公開部が乱数ｒを生成するとともに、この乱数ｒと公開鍵CP_{ITD}で暗号化したデータＣをコンテンツ秘密部に送信する（ステップＳ１５）。

【００９６】コンテンツ秘密部側では、自身が持つコンテンツ秘密鍵CS_{ITD}を用いて暗号データＣを復号化して（ステップＳ１６）、この復号結果Ｒをコンテンツ公開部に返す（ステップＳ１７）。

【００９７】コンテンツ公開部は、コンテンツ秘密部から戻された値Ｒと乱数ｒを比較して、認証を行う（ステップＳ１８）。

【００９８】図５及び図６に示す例では、コンテンツ保持装置１０は、このコンテンツを複製されないためには、少なくともコンテンツ秘密部のみをハードウェア機構を利用して保護し、さらに、コンテンツ確認のうち少なくともコンテンツ秘密部を用いてレスポンス値を計算する手順については不正解析に耐久性のあるハードウェア上で行うようにする。コンテンツ保持装置間でコンテンツ譲渡を行う度に、上述したようなコンテンツ確認を行うことで、改竄のないコンテンツのみが流通することを保証することができる。

【００９９】本実施形態ではさらに、コンテンツに一定の期限があり、ある一定期間の後にその大部分が回収されると想定する。ここで言う「回収」とは、コンテンツの発行者あるいはその代理人であるコンテンツ回収者の元にコンテンツが集められることを意味する。この回収は、コンテンツの有効期限による方法、例えばコンテンツが電子チケットである場合のように、特定日時に有効でその際に回収する方法などが考えられる。例えば改札に相当するコンテンツ回収装置５０においてコンテンツの回収が行われる。

【０１００】３．コンテンツ保持装置

本発明を適用するコンテンツ保持装置１０としては、ここでは以下の説明を簡単にするために、コンテンツの保持装置全体がハードウェア的に耐久性があるＩＣカードの場合を例にとって説明する。ＩＣカードは、解析が困難なように設計・制作されており、通常はカード内部に保持されている情報を読み出すことができない。

【０１０１】図７には、本発明に適用可能なコンテンツ保持装置１０の構成を模式的に示している。同図に示すように、コンテンツ保持装置１０は、コンテンツ送受信部１１と、メモリ部１２と、認証処理部１３と、電子署名検証部１４と、暗号処理部１５と、電子署名生成部１６と、固有情報保持部１７とで構成される。

【０１０２】コンテンツ送受信部１１は、他のコンテンツ保持装置１０や、コンテンツ発行装置、コンテンツ回収装置との間で、コンテンツを譲渡又は譲受するための機器間データ通信を行う。コンテンツの授受は、所定の認証手続を経た後に行われるが、その詳細は後述に譲る。

【０１０３】メモリ部１２は、電子チケットなどのコンテンツや、乱数、譲渡履歴（後述）などの機器間認証処理に使用される作業データなどを保持する。

【０１０４】暗号処理部１５は、共通鍵暗号アルゴリズム（前述）を用いた暗号化・復号化の処理を行う。

【０１０５】認証処理部１３は、コンテンツを授受する相手（他のコンテンツ保持装置１０や、コンテンツ発行装置３０、コンテンツ回収装置５０など）が正しくシステムに属する装置であるかを確認するための機能を持つ。この認証処理には、各装置が生成する電子署名や、管理センタ（ＣＡ）７０による署名証明書を利用することができる。

【０１０６】固有情報保持部１７は、コンテンツ保持装置１０の署名証明書（$Info_k$，P_k，SG_k）と、この証明書に含まれる公開鍵P_kに対応する秘密鍵S_k、並びに、管理センタＣＡ７０の公開鍵P_{CA}、コンテンツ保持装置１０の固有番号ＨＩＤ$_k$などの認証処理に使用される固有情報が保持される。

【０１０７】電子署名生成部１６は、自身の秘密鍵S_kを用いて自分の電子署名を生成する機能を持つ。データＭが存在するとき、電子署名生成部１６は自分の秘密鍵S_kを用いて、電子署名ＳＧ（Ｍ）＝Ｄ（S_k，ｈ（Ｍ））を計算する。データＭを送る際に（Ｍ，ＳＧ（Ｍ））の組で送る（前述）。

【０１０８】また、電子署名検証部１４は、他のコンテンツ保持装置１０、コンテンツ発行装置３０、コンテンツ回収装置５０、並びに、管理センタＣＡ７０の電子署名を検証する機能を持つ。電子署名検証部１４は、ｈ（Ｍ）＝Ｅ（P_k，ＳＧ（Ｍ））が満たされるかどうかを確認することで、Ｍが改竄されていないことと、電子署名ＳＧ（Ｍ）が秘密鍵S_kの所有者によって付加されたものであることを確認する（前述）。

【０１０９】勿論、本発明を実現する上で、コンテンツ保持装置１０はＩＣカードのみに限定されるものではない。例えば、特開平１１－３２８８５０号公報に開示された情報配信システムや、特願２０００－３７８２６１号明細書に開示された電子チケット・システムを、本実施形態に係るコンテンツ保持装置１０として想定することも可能である。

【０１１０】４．コンテンツ発行装置

本実施形態で言う「コンテンツ」は、例えば、乗車券、入場券、会員所、許可書、サービス券などに関する電子チケットを意味する。したがって、本実施形態に係るコンテンツ発行装置３０は、電子チケットとしてのコンテンツを最初に生成する装置である。

【０１１１】コンテンツ発行装置３０は、コンテンツ発行者に相当し、コンテンツとして保持されるべき情報を入力として受け付けて、これらの情報をコンテンツとして一時保持し、さらにコンテンツ保持装置１０にコンテンツを譲渡する機能を持つ。但し、コンテンツを譲受したり回収する機能は持たない。

【０１１２】図８には、本発明に適用可能なコンテンツ発行装置３０の構成を概式的に示している。同図に示すように、コンテンツ発行装置３０は、コンテンツ送受信部３１と、メモリ部３２と、認証処理部３３と、電子署名検証部３４と、暗号処理部３５と、電子署名生成部３６と、固有情報保持部３７と、コンテンツ生成部３８で構成される。

【０１１３】コンテンツ生成部３８は、コンテンツとして保持されるべき情報を入力として受け付けて、電子チケットなどに相当するコンテンツを生成する。コンテンツとして保持されるべき情報としては、例えば、コンテンツ固有の識別情報ＴＩＤや、コンテンツ発行者による電子署名ＣＳＧ、管理センターＣＡ７０から取得したコンテンツ発行者の署名証明書などである。生成されたコンテンツは、例えば、図３又は図５に示すデータ構造を持つ。

【０１１４】コンテンツ送信部３１は、コンテンツ保持装置１０に対してコンテンツを譲渡するための機器間データ通信を行う。ここで言うコンテンツの譲渡は、電子チケットなどに相当するコンテンツの販売に相当する。

【０１１５】メモリ部３２は、電子チケットなどのコンテンツや、乱数、譲渡属歴（後述）などの機器間認証処理に使用される作業データなどを保持する。

【０１１６】暗号処理部３５は、共通鍵暗号アルゴリズム（前述）を用いた暗号化・復号化の処理を行う。

【０１１７】認証処理部３３は、コンテンツを授受する相手であるコンテンツ保持装置１０が正しくシステムに属する装置であるかを確認するための機能を持つ。認証処理には、各装置が生成する電子署名や、管理センタ（ＣＡ）７０による署名証明書を利用する。

【０１１８】固有情報保持部３７は、コンテンツ発行装置３０の署名証明書（$Info_i$，P_i，SG_i）と、この証明書に含まれる公開鍵P_iに対応する秘密鍵S_i、並びに、管理センタＣＡ７０の公開鍵P_{CA}、コンテンツ発行装置３０の固有番号ＨＩＤ$_i$などの認証処理に使用される固有情報が保持される。

【０１１９】電子署名生成部３６は、自身の秘密鍵S_iを用いて自分の電子署名を生成する機能を持つ。データＭが存在するとき、電子署名生成部３６は自分の秘密鍵S_iを用いて、電子署名ＳＧ（Ｍ）＝Ｄ（S_i，ｈ（Ｍ））を計算する。データＭを送る際に（Ｍ，ＳＧ（Ｍ））の組で送る（前述）。

【０１２０】また、電子署名検証部３４は、コンテンツ保持装置１０や管理センタＣＡ７０の電子署名を検証する機能を持つ。電子署名検証部１４は、ｈ（Ｍ）＝Ｅ（P_k，ＳＧ（Ｍ））が満たされるかどうかを確認することで、Ｍが改竄されていないことと、電子署名ＳＧ（Ｍ）が秘密鍵S_kの所有者によって付加されたものであることを確認する（前述）。

【０１２１】５．コンテンツ回収装置

本実施形態で言うコンテンツの回収とは、例えば、乗車券、入場券、会員所、許可書、サービス券などに関する電子チケットを所定の改札において回収することを意味する。また、本実施形態では、図１に示したように、複

数のコンテンツ保持装置１０間でやり取りされたコンテンツを最後に回収する装置として、コンテンツ回収装置５０を想定する。

【００１２】コンテンツ回収装置５０は、改札に相当し、受け取ったコンテンツの表示や検査する機能を持つ。さらに、回収したコンテンツに対して、後述する不正検出と特定を行う。コンテンツ回収装置５０は、他の装置にコンテンツを譲渡する機能は持たない。コンテンツ回収者だけが所持する。

【００１３】図９には、本発明に適用可能なコンテンツ回収装置５０の構成を模式的に示している。同図に示すように、コンテンツ回収装置５０は、コンテンツ受信部５１と、メモリ部５２と、認証処理部５３と、電子署名検証部５４と、暗号処理部５５と、電子署名生成部５６と、固有情報保持部５７と、コンテンツ回収部５８、不正検出部５９で構成される。

【００１４】コンテンツ受信部５１は、コンテンツ保持装置１０からコンテンツを譲受するための機器間データ通信を行う。ここで言うコンテンツの譲受は、電子チケットなどに相当するコンテンツの回収に相当する。回収したコンテンツは、コンテンツ回収部５８に蓄積される。

【００１５】メモリ部５２は、電子チケットなどのコンテンツや、乱数、譲渡履歴（後述）などの機器間認証処理に使用される作業データなどを保持する。

【００１６】暗号処理部５５は、共通鍵暗号アルゴリズム（前述）を用いた暗号化・復号化の処理を行う。

【００１７】認証処理部５３は、コンテンツを譲受する相手であるコンテンツ保持装置１０が正しくシステムに属する装置であるかを確認するための機能を持つ。認証処理には、各装置が生成する電子署名や、管理センタ（ＣＡ）７０による署名証明書を利用する。

【００１８】固有情報保持部５７は、コンテンツ発行装置３０の署名証明書（Inf_{03}，P_j，SG_j）と、この証明書に含まれる公開鍵P_jに対応する秘密鍵S_j、並びに、管理センタＣＡ７０の公開鍵P_{ca}、コンテンツ回収装置５０の固有番号ＨＩＤ$_j$などの認証処理に使用される固有情報が保持される。

【００１９】電子署名生成部５６は、自身の秘密鍵S_jを用いて自分の電子署名を生成する機能を持つ。データＭが存在するとき、電子署名生成部５６は自分の秘密鍵S_jを用いて、電子署名ＳＧ（Ｍ）＝Ｄ（S_j，ｈ（Ｍ））を計算する。データＭを送る際に（Ｍ，ＳＧ（Ｍ））の組で送る（前述）。

【００２０】また、電子署名検証部５４は、コンテンツ保持装置１０や管理センタＣＡ７０の電子署名を検証する機能を持つ。電子署名検証部５４は、ｈ（Ｍ）＝Ｅ（P_k，ＳＧ（Ｍ））が満たされるかどうかを確認することで、Ｍが改竄されていないことと、電子署名ＳＧ（Ｍ）が秘密鍵S_kの所有者によって付加されたものであることを確認する（前述）。

【００２１】不正検出部５９は、コンテンツ受信部５１においてコンテンツ保持装置１０から譲受し、コンテンツ回収部５８に格納された回収コンテンツを検査して、複数のコンテンツ保持装置１０間でコンテンツの授受が繰り返される仮定で不正が行われなかったかを検証する機能を持つ。不正検出部５９は、例えばコンテンツの譲渡履歴を解析することによって、コンテンツ流通過程において不正行為が行われたことを検出したり、さらに不正行為が行われたコンテンツ保持装置を特定することが可能である。但し、不正検出処理の詳細については後述に譲る。

【００２２】６．コンテンツの譲渡手続　－　譲渡履歴なしの場合

上述した各装置１０，３０，５０間でコンテンツが移動することをコンテンツの「譲渡」と呼ぶ。本実施形態では、装置間でコンテンツが移動する場合、コンテンツは暗号化されてやり取りされる。さらに、コンテンツを、やり取りすべきでない装置以外に渡したり、受け取ったりすることを防ぐために、他の装置との接続時には相互認証が行われる。

【００２３】コンテンツの譲渡側及び譲受側の装置間での認証は、例えば同じシステムに属することが同じ共通鍵Ｋを保持することで確認することができる。図１０には、装置間で行う認証手続の処理手順を模式的に示している。同図中で、ａ，ｂは、認証の開始側装置（ａ）と受け側装置（ｂ）のどちらで暗号化されたかを区別するために、あらかじめ決まっている数値である。また、システムに属するすべてのコンテンツ保持装置１０で共有されている。また、ｒ１ａは、数値ｒａのビット連結を意味する。また、コンテンツの譲渡側の装置はコンテンツ保持装置１０又はコンテンツ発行装置３０であり、コンテンツの譲受側の装置は他のコンテンツ保持装置１０又はコンテンツ回収装置５０である。

【００２４】まず、認証の開始側の装置が乱数ｒ１を発生して、認証の受け側の装置に転送する。

【００２５】これに対し、受側の装置は、受信した乱数ｒ１とあらかじめ定められた値ｂとをビット連結して、これを共通鍵Ｋで暗号化して、暗号文ｃｒ１（＝Ｅ（Ｋ，ｒ１｜ｂ））を生成する。受側の装置は、さらに乱数ｒ２を生成して、暗号文ｃｒ１とともに開始側の装置に返信する。

【００２６】開始側の装置は、受信した暗号文ｃｒ１を共通鍵で復号化して平文Ｒ１（＝Ｄ（Ｋ，ｃｒ１））を生成する。そして、Ｒ１とｒ１｜ｂを比較して、両者が一致したならば、受側の装置を認証成立する。開始側の装置は、さらに、受信した乱数ｒ２をあらかじめ定められた値ａ（ａはｂとは異なる）とビット連結して、これを共通鍵Ｋで暗号化して、その暗号文ｃｒ２（＝Ｅ（Ｋ，ｒ２｜ａ））を受側の装置に送信する。

【0137】受け側の装置は、受信した暗号文ｃｒ2を共通鍵で復号化して平文R2(=D(K，ｃｒ2))を生成する。そして、R2とｒ2|ａを比較して、両者が一致したならば、開始側の装置を認証成立する。

【0138】図10に示したような認証を通過することができるのは、同一システム内で共有される共通鍵Kを持っている装置に限られる。したがって、この共通鍵Kを同じシステムに属するコンテンツ保持装置10すなわちICカードだけが共有しているとすれば、上述した認証を経ることによって、お互いが同一システムに属することを確認することができる。この手順のことを、以降の説明では「認証手続き」と呼ぶことにする

【0139】上述したような認証手続がコンテンツの譲渡側及び譲受側の装置間で成功裏に終了すると、譲渡側の装置は、メモリ部12内のコンテンツを暗号化して譲受側の装置に転送する。

【0140】図11には、認証手続の後に、コンテンツの譲渡側及び譲受側の装置間で行うコンテンツの転送手続を模式的に示している。

【0141】まず、コンテンツ譲渡側の装置は、コンテンツの暗号化用の鍵として用いる乱数K_2を新たに生成する。そして、このコンテンツ暗号化鍵K_2をコンテンツ譲受側の装置と共有するために、暗号化鍵K_2をシステム内で共有される共通鍵Krで暗号化した暗号文ｃｋｒ(=E(K，K_2))をコンテンツ譲受側の装置に転送する。

【0142】次いで、コンテンツ譲渡側の装置では、電子チケットなどの送るべきコンテンツCnを共有された鍵Krで暗号化して、その暗号文ｃｃｎをコンテンツ譲受側の装置に転送する。

【0143】これに対し、コンテンツ譲受側の装置では、受け取った暗号文ｃｃｎを共有された鍵Krで復号化して、元のコンテンツCnを得る。次いで、コンテンツ譲受側の装置は、このコンテンツCnについてコンテンツ確認を行う。

【0144】コンテンツが図3に示すようなデータ構造を持つ場合には、そのコンテンツ確認は、図4にフローチャート形式で示した処理手順に従い、署名証明書Ｃｅｒｔの確認、管理センタCA70の公開鍵P_{C8}を用いた署名証明書Ｃｅｒｔの検証、署名証明書Ｃｅｒｔから抽出したコンテンツ発行者の公開鍵P_3を用いた電子署名CSGの検証によって行われる（前述）。あるいは、コンテンツが図5に示すように秘密部と公開部とに分かれたデータ構造を持つ場合には、そのコンテンツ確認は、署名証明書Ｃｅｒｔの確認、管理センタCA70の公開鍵P_{C8}を用いた署名証明書Ｃｅｒｔの検証、署名証明書Ｃｅｒｔから抽出したコンテンツ発行者の公開鍵P_3を用いた電子署名CSGの検証によってコンテンツ公開部の正当性を確認した後に、チャレンジ・レスポンス認証によってコンテンツ秘密部の正当性を確認することによって行われる（前述）。

【0145】コンテンツ譲受側の装置は、コンテンツ確認に成功すると、コンテンツの受け入れをコンテンツ譲渡側の装置に通知する。これに応答して、コンテンツ譲渡側の装置では、メモリ部12に格納されている元のコンテンツC_nを削除する。また、コンテンツ譲受側の装置では、復号化されたコンテンツC_nを自分のメモリ部12に追加する。

【0146】メモリ部12内のコンテンツを暗号化して転送することでコンテンツの移動を行う手順を、以下の説明では「コンテンツ転送」と呼ぶことにする

【0147】なお、コンテンツの譲渡などのデータ転送には通信エラーへの対策が本来は必要であるが、この点は本発明の要旨とは直接関連しないので、本明細書では説明を省略する。

【0148】7．譲渡履歴の構造

本実施形態では、コンテンツを複数の装置間で授受を繰り返す過程で不正の行われた装置を特定するために、各コンテンツにコンテンツ保持装置間でのやり取りの履歴を記録する「譲渡履歴」をさらに用意する。

【0149】譲渡履歴とは、コンテンツの譲渡の履歴を記録した情報のことである。図12は譲渡履歴のデータ構造の一例を示している。図示の譲渡履歴は、コンテンツの固有番号であるＴＩＤと、1回のコンテンツ譲渡手続が行われる毎に1つずつ追加されるレコード（レコード1，レコード2，…）とで構成される。

【0150】最初のレコードすなわちレコード1は、コンテンツ発行装置10からコンテンツ保持装置10Aへコンテンツが譲渡されたという譲渡履歴を示す。同様に、n番目のレコード（レコードn）は、（n－1）番目のコンテンツ保持装置からn番目のコンテンツ保持装置へコンテンツが譲渡されたという譲渡履歴を示す。

【0151】n番目のレコードすなわちレコードnは、コンテンツ譲渡の際におけるコンテンツ譲渡側の装置の固有番号ＨＩＤであるSID_n（Sender ID）と、コンテンツ譲受側の装置の固有番号ＨＩＤであるRID_n（Receiver ID）と、時刻や乱数などからなる1回限りの数（ノンス）であるN_nと、コンテンツ譲渡側の装置が生成したデジタル署名であるTSG_nとで構成される。

【0152】TSG_nは、譲渡履歴の全体に対するデジタル署名である つまり、ＴＩＤとレコード1からレコードnまでのすべて（但し、レコードnのデジタル署名TSG_nの部分は0とする）に対するデジタル署名とする。すなわち、ＴＩＤとレコード1からレコードnまでのすべて（TSG_nの部分は0）をデータM_nとおくと、TSG_nは$D(S_n, h(M_n))$と表される（但し、S_nはn番目にコンテンツ譲渡を行うコンテンツ保持装置の秘密鍵とする）。

【0153】譲渡履歴は、コンテンツ自体と異なり、唯一性を保つ必要はない。したがって、コンテンツ自体と

は分けて、コンテンツ保持装置１０のユーザが読み書きできる記憶領域に保持することが可能である。但し、ユーザが不用意に改変を行った場合には、後述するコンテンツ譲渡の手続きで譲渡履歴交換が成功しなくなるので、そのようなことが容易に行われないように保持されることが望ましい

【０１５４】８．コンテンツの譲渡手続　－　譲渡履歴を使用した場合

譲渡履歴を使用しない場合のコンテンツの譲渡手続については既に説明したので、ここでは、譲渡履歴を使用した場合のコンテンツの譲渡手続について説明する。

【０１５５】コンテンツを交換する過程で譲渡履歴を取り扱う場合、コンテンツ保持装置１０は、譲渡履歴の検証や譲渡履歴の更新を行う譲渡履歴管理部１８を備えている（図２０を参照のこと）。また、コンテンツ発行装置３０は、コンテンツの譲渡時に譲渡履歴を生成する譲渡履歴生成部３９を備えている（図２１を参照のこと）。また、コンテンツ回収装置５０における不正検出部５９は、譲渡履歴の各レコードを解析してコンテンツ流通過程における不正を検出する機能を備えている。

【０１５６】図２２には、譲渡履歴を加えた場合における、コンテンツ保持装置間でのコンテンツ譲渡を行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って、譲渡履歴を利用したコンテンツ譲渡手続について説明する。

【０１５７】譲渡履歴を加えた場合のコンテンツの移動においては、まず、コンテンツ保持装置間で認証手続を行う（ステップＳ５１，Ｓ５２）。装置間の認証手続については、既に図１０を参照しながら説明したので、ここでは説明を省略する。

【０１５８】装置間の認証手続に成功した場合には、次いで、譲渡履歴の受け渡しを行なう譲渡履歴交換が行われる（ステップＳ５３，Ｓ５４）。但し、以下のデジタル署名認証から、コンテンツを交換する相手機の装置が同一システムに属することが確認できるとき、例えば署名証明書が同一のシステムに属するコンテンツ保持装置に対してのみ発行されている場合（すなわち、共通鍵Ｋを保持していることと同じ場合）には、認証手続きに代えて、譲渡履歴交換を行えばよい。譲渡履歴の好感手続の詳細については後述に譲る。

【０１５９】譲渡履歴の交換に成功した後には、上述のコンテンツ転送（図１１を参照のこと）を行う（ステップＳ５５，Ｓ５６）。

【０１６０】そして、コンテンツの転送に成功した後に、譲渡された譲渡履歴とコンテンツの双方に含まれる固有番号ＴＩＤが一致することを確認して、コンテンツの譲渡が完了する（ステップＳ５７）

【０１６１】図１３には、コンテンツの譲渡側と譲受側のコンテンツ保持装置間で行われる譲渡履歴の交換手続について模式的に示している。また、図１４には、この譲渡履歴の交換手続のうち、譲渡側のコンテンツ保持装置から譲受側のコンテンツ保持装置へのデジタル署名認証の処理手順を、フローチャートの形式で示している。（譲受側のコンテンツ保持装置から譲渡側のコンテンツ保持装置へのデジタル署名認証の処理手順は、図１４と同様であるので説明を省略する。）以下、図１３及び図１４を参照しながら、譲渡履歴の交換手続について説明する。

【０１６２】まずコンテンツ譲渡側の保持装置は、自分の署名証明書をコンテンツ譲受側の保持装置に送付する（ステップＳ２１）。署名証明書としては、コンテンツ譲渡側の保持装置と結びつく情報$Ｉｎｆｏ_{n}$と$Ｐ_{n}$を組にしたもの（$Ｉｎｆｏ_{n}$，$Ｐ_{n}$）に、管理センタＣＡ７０が自分の秘密鍵$Ｓ_{CA}$を使って生成した署名$ＳＧ_{r}＝Ｄ（Ｓ_{CA}$，ｈ（$Ｉｎｆｏ_{n}$，$Ｐ_{n}$））を付加した証明書（前述）を使用することができる。

【０１６３】これに対し、コンテンツ譲受側の保持装置では、署名証明書の検証を行う（ステップＳ２２）。管理センタＣＡ７０の公開鍵$Ｐ_{CA}$を用いて証明書の署名確認を行うことによって（ｈ（$Ｉｎｆｏ_{n}$，$Ｐ_{n}$）＝Ｅ（$Ｐ_{CA}$，$ＳＧ_{n}$））、証明書の正当性を検証することができる（前述）。

【０１６４】そして、証明書が正しい場合には、コンテンツ譲受側の保持装置は、乱数ｒを発生して（ステップＳ２３）、この乱数ｒをコンテンツ譲渡側の保持装置に送る（ステップＳ２４）

【０１６５】コンテンツ譲渡側の保持装置では、受け取った乱数ｒに署名$Ｓｇｎ＝Ｄ（Ｓ_{n}$，ｈ（ｒ））を生成して（ステップＳ２５）、これをコンテンツ譲受側の保持装置に返送する（ステップＳ２６）。

【０１６６】コンテンツ譲受側の保持装置では、電子署名Ｓｇｎが自ら発生した乱数ｒに対するコンテンツ譲渡側の保持装置の署名として正しいかどうかを検証する（ステップＳ２７）署名の正当性は、コンテンツ譲渡側の保持装置の公開鍵$Ｐ_{n}$を用いて、ｈ（ｒ）＝Ｅ（$Ｐ_{n}$，Ｓｇｎ）によって検証することができる。

【０１６７】そして、上述と同様に、コンテンツ譲受側の保持装置からコンテンツ譲渡側の保持装置に対してもデジタル署名認証を行うことで、両コンテンツ保持装置はお互いの署名検証鍵とＩＤを正しく把握することができるようなる。コンテンツ譲受側の保持装置のＩＤは、レコードの作成時（後述）に用いられる。

【０１６８】次いで、コンテンツ譲受側の保持装置では、大きなビット数の乱数や時刻情報から、毎回（コンテンツを譲渡する度に）異なる数ノンスＴ$Ｎ_{n}$を発生し、これをコンテンツ譲渡側の保持装置に送付する

【０１６９】コンテンツ譲渡側の保持装置では、譲渡履歴を更新して、新規レコードを生成する 新規レコードｎは、コンテンツ譲渡の際におけるコンテンツ譲渡側の装置の固有番号$ＳＩＤ_{n}$と、コンテンツ譲受側の装置の

固有番号ＲＩＤ$_{\Sigma}$と、ノンスＴＮ$_{\Sigma}$とで構成される（前述）。

【０１７０】最後に、コンテンツ譲渡側の保持装置は自らの秘密鍵S_{Σ}を使って、新規レコードを含む譲渡履歴全体に対する電子署名ＴＳＧ$_{\Sigma}$を生成し（但し、新規レコード中のＴＳＧ$_{\Sigma}$部分を０として計算する）、新規レコードに追加する（前述）。更新された譲渡履歴は、コンテンツ譲受側の保持装置に送付される。

【０１７１】これに対し、コンテンツ受信側の保持装置では、受信した譲渡履歴の確認を行う すなわち、先行する電子署名の検証手続きを介して把握したコンテンツ譲渡側の保持装置のＩＤが新規レコードのＳＩＤ$_{\Delta}$に、自分のＩＤがＲＩＤ$_{\Sigma}$に正しく含まれること、並びに、先に自身が発生したものと同じノンスＴＮ$_{\Delta}$が含まれることを確認する。そして最後に、コンテンツ譲渡側の保持装置の署名検証鍵P_{Δ}を使って新規レコードの署名ＴＳＧ$_{\Sigma}$が正しく譲渡履歴に対するコンテンツ譲渡側の保持装置の署名になっていることを検証する 署名ＴＳＧ$_{\Sigma}$の検証は、ＴＩＤとレコード１からレコードｎまでのすべて（ＴＳＧ$_{n}$の部分は０）をデータM_{n}とおくと、ｈ（M_{n}）＝Ｄ（P_{Δ}，ＴＳＧ$_{\Sigma}$）によって行うことができる。

【０１７２】コンテンツ譲受側の保持装置での譲渡履歴の確認が成功した場合には、コンテンツ譲渡側の保持装置では元の譲渡履歴を削除し、コンテンツ譲受側の保持装置では受け取った譲渡履歴を保存して、譲渡履歴交換が終了する

【０１７３】９．不正検出と特定

上述したコンテンツ譲渡手続き（図１１を参照のこと）を行うことで、各コンテンツには、コンテンツの発行者（発行装置３０）から現在のコンテンツ所有者（保持装置１０）までの譲渡の履歴が記録された譲渡履歴（図１２を参照のこと）が付属することになる。

【０１７４】各コンテンツは唯一性があり、同時には単一のコンテンツ保持装置（ＨＩＤで区別される）でのみ保持されている。各コンテンツ保持装置は装置の固有番号ＨＩＤによって識別可能であるので、固有番号ＴＩＤで識別される各特定のコンテンツの譲渡履歴は一種類であるべきである。

【０１７５】ところが、ハードウェアの不正解析が行われコンテンツが複製された場合を想定すると、あるＴＩＤを割り当てられたコンテンツが複数のコンテンツ保持装置上に同時に保持されるようになり、この結果、不正行為が行なわれたＴＩＤに対して複数の譲渡履歴が生じる。

【０１７６】ここで、譲渡履歴が完全である場合、すなわちコンテンツ保持装置１０の解析によりコンテンツの不正複製が行われたとしても、譲渡履歴は上述した手順で正しく記録される場合（譲渡履歴は改竄が不可能である場合）について考察してみる。

【０１７７】最初にコンテンツ発行者はコンテンツが唯一になるように発行するので、これらの譲渡履歴は不正を行ったコンテンツ保持装置に到達するまでは、唯一のコンテンツとともに単一の譲渡履歴のみが存在する。しかし、不正が行われたコンテンツ保持装置からの譲渡に対応するレコードはそれぞれ異なり、以降は異なる譲渡履歴になる。以下では、これを譲渡履歴の「枝分かれ」と呼び、枝分かれの発生したレコードを「枝分かれレコード」と呼ぶことにする。譲渡履歴の枝分かれによって、不正が行われて複製されたコンテンツに対しては複数種類の譲渡履歴が生じる。

【０１７８】不正によってコンテンツが複製されると、有効期限切れや改札などコンテンツ回収装置５０によるコンテンツ回収によって、特定のコンテンツ（すなわち、特定のＴＩＤ）が複数回回収されることになる。まず、単一のＴＩＤが２回以上回収されたということから、コンテンツが譲渡される途中で不正が行われたことが判明する。

【０１７９】さらに、このコンテンツ複製による譲渡履歴の枝分かれに対応して、複数種類の譲渡履歴が回収されることになる。この回収された複数の譲渡履歴を解析して、枝分かれレコードを探すことで、そのレコードの送り側ＩＤすなわちＳＩＤのコンテンツ保持装置を不正の行われたコンテンツ保持装置として特定することができる。

【０１８０】以上の説明では、譲渡履歴の完全性が保たれていることを前提としている。しかしながら、本発明はこのような前提に拘束されるものではなく、この譲渡履歴がコンテンツの不正複製を行うようなコンテンツ保持装置でどのように改変されても、不正を行ったコンテンツ保持装置を特定することができる。

【０１８１】以下では、不正には譲渡履歴を改竄することを含めて、不正を行なったコンテンツ保持装置を特定する場合について説明する。併せて、不正を行うコンテンツ保持装置が複数あり且つそれらが共謀する場合であっても、不正を行った複数のコンテンツ保持装置のうち少なくとも１つを特定できることを示す。

【０１８２】１０．不正特定の仮定

譲渡履歴の不正改竄や、複数のコンテンツ保持装置の共謀を検出する上で、以下の２点を仮定する。すなわち、（１）不正によって可能になるのは、自分あるいは仲間の所有するコンテンツ保持装置に保持されているコンテンツの複製、及び、そのコンテンツ保持装置のデジタル署名の生成である。

（２）コンテンツの譲渡履歴を改竄できるのは、譲渡履歴が自分のコンテンツ保持装置ないに保持されている期間だけである。すなわち、他人が保持している譲渡履歴は改竄できない。

【０１８３】これらの仮定はコンテンツの譲渡履歴に基づく不正行為の検出を実装する上で現実的な条件である

ということを、当業者であれば容易に理解できるであろう。

【０１８４】１１．不正検出と不正者特定の手順

コンテンツの譲渡履歴を利用した不正検出、及び不正コンテンツ保持装置の特定は、以下に示す４段階の手順によって構成される。また、図１５には、コンテンツの譲渡履歴を利用して不正検出、及び不正コンテンツ保持装置を特定するための処理手順をフローチャートの形式で示している。以下、このフローチャートを参照しながら、不正検出と不正者特定の手順について説明する。

【０１８５】（１）同じ固有番号ＴＩＤを持つコンテンツが複数回回収されていないかどうかを検査する（ステップＳ３１）。もし、ＴＩＤの異なるすべてのコンテンツが１回ずつしか回収されていなければ、不正は行われていないので、本処理手順を終了する。他方、同じＴＩＤを持つコンテンツが２回以上回収された場合には、その譲渡履歴を集めて、ＴＩＤ毎に手順（２）以降の処理を行う。

【０１８６】（２）ＴＩＤが同じそれぞれの譲渡履歴について、含まれるすべてのレコードについて新しいものから古いものに辿りながら電子署名TSG_nを検証する（ステップＳ３４～Ｓ３７）。途中で電子署名が正しくないレコードｋが見つかった場合、その次のレコードｋ＋１の送り側（つまり検証できないレコードを受け入れた装置）で不正が行われたことになる（ステップＳ４３）。手順（２）で不整合が見つからない譲渡履歴については、次の手順（３）に進む。

【０１８７】（３）ＴＩＤが同じそれぞれの譲渡履歴について、譲渡履歴の先頭レコード（すなわち最も古いレコード）のコンテンツ譲渡側となった装置（ＳＩＤ）が、当該コンテンツすなわちチケットの発行者（HID_{ISSUER}）か否かを判断する（ステップＳ３８）。先頭レコードのコンテンツ譲渡側となった装置（ＳＩＤ）がチケットの発行者（HID_{ISSUER}）でない場合、このコンテンツ譲渡側の装置が不正を行ったコンテンツ保持装置の番号になる（ステップＳ４４）。そうでない譲渡履歴、すなわち単体の譲渡履歴からは不正が特定できないものについては、一旦プールしておく（ステップＳ３９）。その上で、処理中のＴＩＤで他に未処理の譲渡履歴があれば、そちらについても上記の手順（２）及び（３）を実行する（ステップＳ４０）。同一のＴＩＤを持つすべての譲渡履歴について処理が終わったならば、次の手順（４）に進む。

【０１８８】（４）プールされている同一ＴＩＤの譲渡履歴が複数存在する場合には、互いの譲渡履歴を比較して、それらの枝分かれレコードを探す。枝分かれレコードにおけるコンテンツ譲渡側のコンテンツ保持装置（ＳＩＤ）が不正を行ったことになる（ステップＳ４１）。

【０１８９】１２．不正者を特定できることの証明

ここで、上記の「１１．不正検出と不正者特定の手順」によって不正者を特定することができること、すなわち、不正を行っていない者が誤って不正者に特定されることがないことを証明しておく。

【０１９０】上述した手順（１）は、不正の検出である。

【０１９１】また、上述した手順（２）では、譲渡履歴に含まれるレコードに不整合がある場合、その不整合から改竄を行った者を特定する。以下、この特定手順が成功することを、コンテンツ保持装置が正しく動作し、上記コンテンツ譲渡手順が正しく行われる限り、誤って不正が行われたコンテンツ保持装置と特定されないことを示し、その対偶として証明する。

【０１９２】あるコンテンツ保持装置（HID_{n-1}）から別のコンテンツ保持装置（HID_n）にコンテンツすなわち電子チケットが譲渡される際に追加されたレコードｎには、HID_{n-1}の電子署名が付加されている（前述）。手順（３）により、コンテンツ保持装置HID_nはこの電子署名を検証し、整合性がない場合には受け取りを拒否するはずである。したがって、仮定（２）、並びに、コンテンツ保持装置ＨＩＤｎ が正しく動作するという前提条件により、正しいレコードｎが追加された譲渡履歴が次のコンテンツ保持装置HID_{n+1}に渡される。ある１つのコンテンツ保持装置HID_nに注目したとき、それが上述した手順（２）で不正とみなされるのは、新しいレコードから辿っていったときに、コンテンツ保持装置HID_nの受け入れたレコードｎではじめて不整合になるときである。しかし、以後のチケット保持者が不正を行わない限り、レコードｎの電子署名が不整合になることはない。

【０１９３】次に、HID_nより後に譲渡を受けるコンテンツ保持装置が不正を行う場合、例えば、固有番号HID_n（ｐ＞ｎ）を持つコンテンツ保持装置が、以前のどれかのレコードを改竄した場合を考え、これによって、レコードｎより以降に追加されたレコードの電子署名の整合性を保ちながら、レコードｎの電子署名の整合性が失われるような改竄の可能性について考察してみる。

【０１９４】レコードｐにはHID_{p-1}の電子署名が付加されており、その電子署名はレコードｐを含む譲渡履歴全体に対するものである。したがって、あるレコードｋ（ｋ＜ｐ）の改竄により、レコードｋの電子署名だけでなく、レコードｋとレコードｐの間のすべてのレコードの電子署名が不整合になる。

【０１９５】HID_pがこの部分のレコードの不整合をすべて解消できるのは、仮定（１）により、それらのレコードに電子署名したコンテンツ保持装置がすべて自分あるいは仲間の所有である場合に限られる。前提条件から、コンテンツ保持装置HID_nは正しく動作するので、レコードｎ＋１に含まれるコンテンツ保持装置HID_nの電子署名の整合性を取ることはできない。したが

って、レコードkとレコードpの間にレコードnが含まれる場合、レコードn を不整合とし、レコードn+1以降が整合性を保つような改変を行うことはできないことが分かる。

【0196】上述した手順（3）では、議渡履歴の各レコードに関して整合性が保たれるような改竄について扱う。上述した通り、コンテンツ保持装置HID_pが過去のレコードkを改変した場合、レコードkからレコードpまでのすべてのレコードが不整合となる。仮定（1）より、コンテンツ保持装置HID_pはこのうちで過去に自分又は共謀者が生成した履歴レコードのみに整合性を持たせることができる。このため、コンテンツ保持装置HID_gにできることは、こうした履歴レコードR_qを改変してそれ以降の整合性の取れない履歴レコードを捨て去るか、又は、既存の履歴レコードをすべて捨て去ってコンテンツ保持装置HID_pが議渡履歴の最初のレコードを作成することである。前者の場合は検出できない。後者の場合は、先頭レコードが示す送り側の装置がコンテンツすなわち電子チケットの発行者の電子署名と異なることから検出可能である。

【0197】これまでの議論をまとめると、過去に不正者あるいはその共謀者が生成した履歴レコードを改変し、それ以降のレコードを削除した場合、あるいは議渡履歴の改竄を行わなかった場合以外は、議渡履歴自体の整合性の検査から、不正が検出されることが分かる。

【0198】したがって、コンテンツ保持装置HID_pでコンテンツの複製を行った不正者が、議渡履歴自体の整合性の検査で特定されることを避けたい場合、通常のコンテンツ譲渡を行いレコードp+1を加えるか、又は、過去に不正者あるいはその共謀者が生成した履歴レコードR_qを改変してR_q'とし、R_q以降の譲渡履歴レコードを削除することである。

【0199】上述した手順（4）により、これらの場合が取り扱われる。何故なら、どちらの場合でも、議渡履歴に不正者又はその共謀者の番号がコンテンツ譲渡側となるレコードが含まれ、上記のコンテンツ譲渡をあわせて2回以上行うと、枝分かれレコードとして検出することが可能になる。不正者が同じ相手に譲渡する場合でも、その相手も不正を行っていない限り、この譲渡に対応するレコード中のノンスが各回で一致しないため、枝分かれレコードとして検出される。

【0200】以上から、不正検出と不正者特定の手順（1）～（4）によって、不正の検出と不正者特定ができることが示された。

【0201】13．譲渡履歴の暗号化

ここでは、コンテンツ流通の匿名性についてもう一度取り扱う。

【0202】既に述べたように、各装置の所有者とコンテンツ保持装置の固有番号であるHID_1との対応は、管理センタCA70だけが把握しているとすることにより、管理センタCA70以外の通常の利用者に対しては、コンテンツ流通の匿名性が守られる。

【0203】しかしながら、場合によっては特定の保持装置（特定個人と対応すること等価）で、どのようなコンテンツが保持されていたかの記録を収集することが重要な情報となりうる。また、何らかの方法によって装置の固有番号HID_1と利用者の対応関係が特定された場合、譲渡履歴はある特定個人がどのようなコンテンツを好むかといったことを知るための手がかりとなってしまい、コンテンツ利用者のプライバシが脅害されるおそれがある。

【0204】このような場合に対処するために、管理センタCA70とコンテンツ譲渡の当事者以外は譲渡履歴を参照できなくする方法について、以下に説明する。そのためにまず、管理センタCA70は公開鍵暗号の公開鍵及び秘密鍵のペアを生成する。ここでは、管理センタCA70の公開鍵をP_{CA}とし、その秘密鍵をS_{CA}とする。管理センタCA70は公開鍵P_{CA}だけを公開する。そして、利用者はこの公開鍵P_{CA}を使って譲渡履歴を暗号化することで、管理センタCA70のみが譲渡履歴を参照できるようにする。

【0205】公開された鍵P_{CA}は、例えば、コンテンツ中に改変されないように含ませればよい。図16には図3に示した構成のコンテンツ中に公開鍵P_{CA}を含ませた様子を示し、また、図17には図5に示した構成のコンテンツ中の公開鍵P_{CA}を含ませた様子を示している。また、譲渡履歴は、図18に示すように、コンテンツの識別番号TID以外のすべてのレコードがP_{CA}を用いて暗号化された状態で流通する。

【0206】図19には、このように譲渡履歴を暗号化した場合のコンテンツ譲渡の手順を模式的に示している。この場合、図13を参照しながら既に説明した「譲渡履歴あり」の場合のコンテンツ譲渡手順と同様の処理手順を踏めばよい。但し、譲渡履歴更新において、コンテンツ譲渡側のコンテンツ保持装置によって生成された新規レコードに含まれる電子署名は、以前の譲渡に対応する暗号化されたレコードを含んだ譲渡履歴全体に対するものとする。譲渡履歴は、追加された新規レコードが暗号化されないままでコンテンツ譲受側のコンテンツ保持装置に返される。

【0207】コンテンツ譲受側のコンテンツ保持装置では、譲渡履歴の確認において、新規レコードに含まれる電子署名を検証する。そして、検証が成功裏に終了した後に、新規レコードを管理センタCA70の公開鍵P_{CA}を用いて暗号化して、譲渡履歴の最後尾の暗号化されていない新規レコードをそれで置換する。

【0208】次いで、不正検出と不正者特定について説明する。但し、不正者は、コンテンツの複製を行なった者、譲渡履歴の改竄を行なった者、並びに、管理センタCA70の公開鍵P_{CA}を用いて譲渡履歴レコードを正し

く暗号化しなかった者とする。

【0209】不正検出と不正者特定の手順は、既に説明した手順と同様でよい。但し、手順（2）において譲渡履歴に含まれるレコードを検証する際に、管理センタCA70の秘密鍵S_{CA}を用いて各レコードを復号化する作業が加わる。この秘密鍵S_{CA}によって正しく復号化できること、及び、レコード中の電子署名が正しいことによって各レコードの正当性が証明される。

【0210】レコードが正しくない場合、すなわちレコードが正しく復号できないか又は電子署名が正しくない場合には、そのレコードを譲受した側のコンテンツ保持装置、すなわち、当該レコードの次のレコードを送ったコンテンツ保持装置が不正を行ったことを示している。これ以外の点に関しては、譲渡履歴を暗号化しない場合と同様であるので、説明を省略する。

【0211】このように、譲渡履歴の各レコードを管理センタCA70の公開鍵P_{CA}で暗号化した場合、譲渡履歴を所定のシステム管理者以外には読めないようにすることができる。この結果、システム管理者には不正が行われたコンテンツ保持装置の特定を可能としながら、通常のコンテンツ利用者にはあるコンテンツがどのコンテンツ保持装置を経由してきたかを秘密にすることができる。

【0212】「追補」以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。例えば、本発明を実現する上で、特定の暗号アルゴリズムに限定されるものではない。要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0213】

【発明の効果】以上詳記したように、本発明によれば、デジタル情報を耐久性のあるハードウェア上に保持することによって、複数の機器間でデジタル情報の譲渡を繰り返す過程において不正利用から保護することができる。優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0214】また、本発明によれば、デジタル情報を複数の機器間で譲渡を繰り返す過程において、万一ある機器ハードウェアが解析・改変された場合であってもデジタル情報を不正利用から保護することができる、優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0215】また、本発明によれば、ハードウェアの解析・改変によるデジタル情報の不正利用を検出することによってハードウェアの解析・改変への潜在的な意図を抑制することができる、優れた情報処理装置及び方法、並びに記憶媒体を提供することができる。

【0216】本発明によれば、ハードウェアの耐タンパ性を用いて情報コンテンツの複製や改変を防ぐ機能を実現している装置において、ハードウェアの不正解析が行われてコンテンツの複製並びに他の装置に譲渡され流通した場合であっても、それらのコンテンツを回収して検査することで、不正の発生を検出し、さらに不正が行われた装置を特定することができる。

【0217】本発明においてコンテンツの譲渡履歴を検査する機能を実現するために、装置間でのコンテンツのやり取りの度にコンテンツ複製の有無を確認する必要がない。また、装置間でのコンテンツのやり取りの度にコンテンツ複製の有無を確認する必要がないので、コンテンツ授受の際にオンラインの確認などが必要なく、不正検出のために必要な計算機負荷やメモリ容量を軽減することができる。

【0218】不正者がハードウェアの解析・改変の結果として、コンテンツの複製によって利益を得ようとしても、本発明によれば不正なコンテンツ保持装置が特定されその装置の所有者として不正者が特定あるいは絞り込めることから、不正者がハードウェア解析・改変を行う意図を抑制するという効果がある。また、不正者の特定を可能としながら、コンテンツの利用者の匿名性、すなわち誰がどのようなコンテンツを利用したかといったプライバシ情報を守ることができる。

【図面の簡単な説明】

【図1】本発明を適用する対象となる、デジタル情報すなわちコンテンツを複製されないように保持するシステム1の構成を模式的に示した図である。

【図2】コンテンツ保持装置10、コンテンツ発行装置30、コンテンツ回収装置50に対して管理センタ（CA）70が電子署名の証明書を発行する仕組みを模式的に示した図である。

【図3】コンテンツの構成例を示した図である。

【図4】図3に示したコンテンツの改竄がないことを確認するための処理手順を示したフローチャートである。

【図5】コンテンツ確認を行うことができる他のコンテンツ構成例を示した図である。

【図6】図5に示したコンテンツの改竄がないことを確認するための処理手順を示したフローチャートである。

【図7】本発明に適用可能なコンテンツ保持装置10の構成を模式的に示した機能ブロック図である。

【図8】本発明に適用可能なコンテンツ発行装置30の構成を模式的に示した機能ブロック図である。

【図9】本発明に適用可能なコンテンツ回収装置50の構成を模式的に示した機能ブロック図である。

【図10】コンテンツの譲渡側及び譲受側の装置間で行う認証手続（但し、譲渡履歴を用いない場合）の処理手順を説明するための図である。

【図11】コンテンツの譲渡側及び譲受側の装置間で認証手続を経た後に各装置間で行うコンテンツの転送手続

を説明するための図である。

【図１２】譲渡履歴のデータ構造の一例を示した図である。

【図１３】コンテンツの譲渡側と譲受側のコンテンツ保持装置間で行われる譲渡履歴の交換手続を模式的に示した図である。

【図１４】譲渡側のコンテンツ保持装置から譲受側のコンテンツ保持装置へのデジタル署名認証の処理手順を示したフローチャートである。

【図１５】コンテンツの譲渡履歴を利用して不正検出、及び不正コンテンツ保持装置を特定するための処理手順を示したフローチャートである。

【図１６】図３に示した構成のコンテンツ中に公開鍵P_{CA}を含ませた様子を示した図である。

【図１７】図５に示した構成のコンテンツ中に公開鍵P_{CA}を含ませた様子を示した図である。

【図１８】コンテンツの識別番号ＴＩＤ以外のすべてのレコードがP_{CA}を用いて暗号化された状態を示した図である。

【図１９】譲渡履歴を暗号化した場合のコンテンツ譲渡の手順を模式的に示した図である。

【図２０】譲渡履歴の受け渡しを伴うコンテンツの移動を行うタイプのコンテンツ保持装置１０の構成を模式的に示したブロック図である。

【図２１】譲渡履歴の受け渡しを伴うコンテンツの移動を行うタイプのコンテンツ発行装置３０の構成を模式的に示したブロック図である。

【図２２】譲渡履歴を加えた場合にコンテンツ保持装置間でコンテンツを交換するための処理手順を示したフローチャートである。

【符号の説明】

１０…コンテンツ保持装置

１１…コンテンツ送受信部，１２…メモリ部

１３…認証処理部，１４…電子署名検証部

１５…暗号処理部，１６…電子署名生成部

１７…固有情報保持部

１８…譲渡履歴管理部

３０…コンテンツ発行装置

３１…コンテンツ送信部，３２…メモリ部

３３…認証処理部，３４…電子署名検証部

３５…暗号処理部，３６…電子署名生成部

３７…固有情報保持部，３８…コンテンツ生成部

３９…譲渡履歴生成部

５０…コンテンツ回収装置

５１…コンテンツ受信部，５２…メモリ部

５３…認証処理部，５４…電子署名検証部

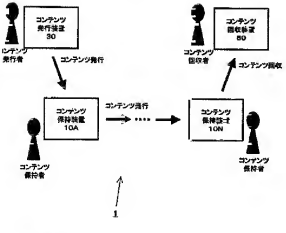
５５…暗号処理部，５６…電子署名生成部

５７…固有情報保持部，５８…コンテンツ回収部

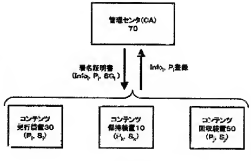
５９…不正検出部

７０…管理センタ（ＣＡ）

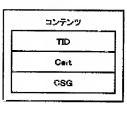
【図１】



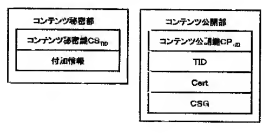
【図２】



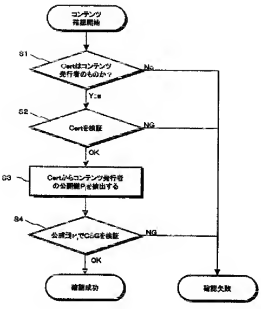
【図３】



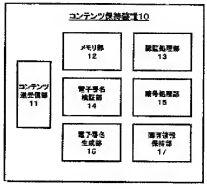
【図５】



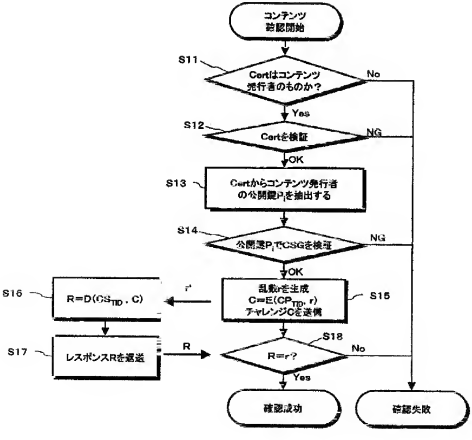
【図4】


コンテンツ
再生開始
S1
Certはコンテンツ
発行者のものか？
No
Yes
S2
Certを検証
NG
OK
S3
Certからコンテンツ発行者
の公開鍵PIを抽出する
S4
公開鍵PIでCSIGを検証
NG
OK
確認成功
確認失敗

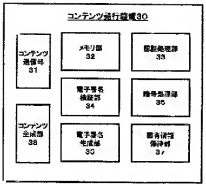
【図7】


コンテンツ受信装置10
コンテンツ
送受信部
11
メモリ部
12
制御処理部
13
署名検証
機能部
14
暗号処理部
15
電子署名
生成部
16
識別情報
保持部
17

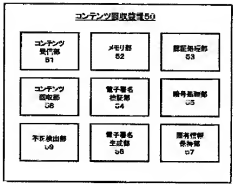
【図6】


コンテンツ
認証開始
S11
Certはコンテンツ
発行者のものか？
No
Yes
S12
Certを検証
NG
OK
S13
Certからコンテンツ発行者
の公開鍵PIを抽出する
S14
公開鍵PIでCSIGを検証
NG
OK
S15
乱数rを生成
C=E(OPID, r)
チャレンジCを送信
r
S16
R=D(GSID, C)
S17
レスポンスRを返送
R
S18
R=r？
No
Yes
確認成功
認証失敗

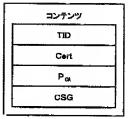
【図8】



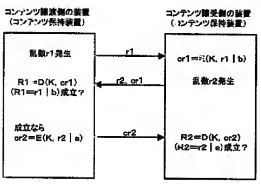
【図9】



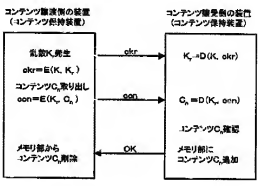
【図16】



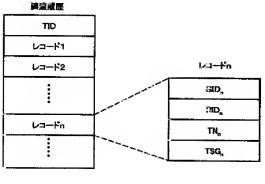
【図10】



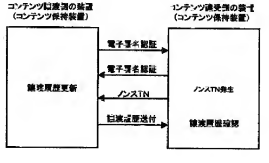
【図11】



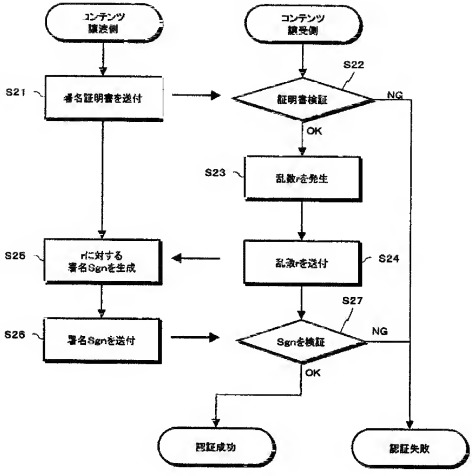
【図12】



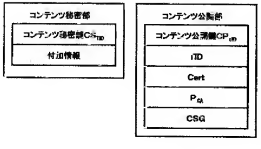
【図13】



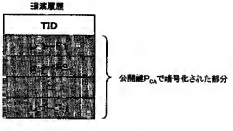
【図14】


コンテンツ
譲渡側
コンテンツ
譲受側
S21
署名証明書を送付
S22
証明書検証
NG
OK
S23
乱数rを発生
S24
乱数rを送付
S25
rに対する
署名Sgnを生成
S26
署名Sgnを送付
S27
Sgnを検証
NG
OK
認証成功
認証失敗

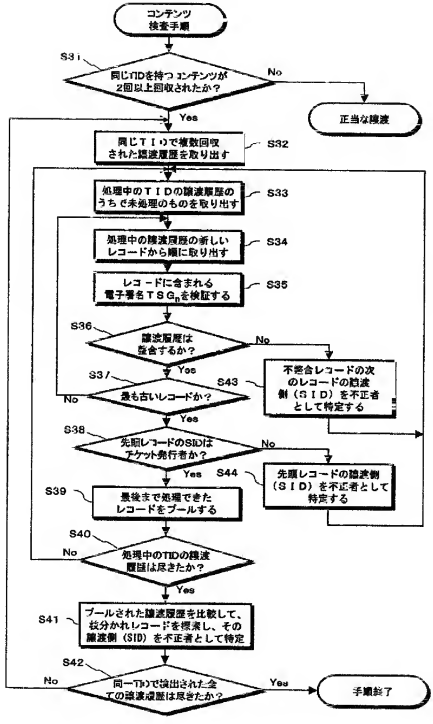
【図17】


コンテンツ格密部
コンテンツ暗号鍵CK
付加情報
コンテンツ公開部
コンテンツ公開鍵CP
TID
Cert
CSG

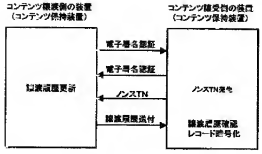
【図18】


非実屋屋
TID
公開鍵PCAで暗号化された部分

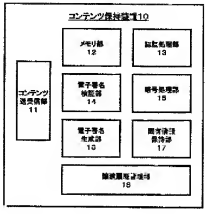
【図15】


コンテンツ
検査手順
S31
同じTIDを持つコンテンツが
2回以上回収されたか？
No
正当な譲渡
Yes
同じＴＩＤで複数回収
された譲渡履歴を取り出す
S32
処理中のＴＩＤの譲渡履歴の
うちで未処理のものを取り出す
S33
処理中の譲渡履歴の新しい
レコードから順に取り出す
S34
レコードに含まれる
電子署名ＴＳＧnを検証する
S35
S36
譲渡履歴は
整合するか？
No
Yes
S37
最も古いレコードか？
No
S43
不整合レコードの次
のレコードの譲渡
側（ＳＩＤ）を不正者
として特定する
Yes
S38
先頭レコードのSIDは
チケット発行者か？
No
Yes
S44
先頭レコードの譲渡側
（ＳＩＤ）を不正者とし
て特定する
S39
最後まで処理できた
レコードをプールする
S40
No
処理中のTIDの譲渡
履歴は尽きたか？
Yes
S41
プールされた譲渡履歴を比較して、
仮分かれレコードを探索し、その
譲渡側（SID）を不正者として特定
S42
No
同一TIDで流出された全
ての譲渡履歴は尽きたか？
Yes
手順終了

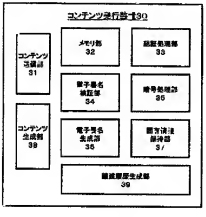
【図19】



【図20】



【図21】



【図22】